Tivoli SecureWay User Administration

Management Handbuch

Version 3.8

Tivoli SecureWay User Administration

Management Handbuch

Version 3.8

Tivoli SecureWay User Administration Management Handbuch
Copyrightvermerk

© Copyright IBM Corporation 2001. Alle Rechte vorbehalten. Kann nur gemäß der Softwarelizenzvereinbarung von Tivoli Systems bzw. IBM oder dem Anhang für Tivoli-Produkte der IBM Nutzungsbedingungen verwendet werden. Diese Veröffentlichung darf ohne vorherige schriftliche Zustimmung der IBM Corporation weder ganz noch in Auszügen auf irgendeine Weise - elektronisch, mechanisch, magnetisch, optisch, chemisch, manuell u. a. - vervielfältigt, übertragen, aufgezeichnet, auf einem Abrufsystem gespeichert oder in eine andere Computersprache übersetzt werden. Die IBM Corporation erteilt Ihnen eine eingeschränkte Berechtigung zur Erstellung einer Hardcopy oder sonstiger Vervielfältigungen in Form maschinenlesbarer Dokumentationen für die interne Verwendung, wobei jede Vervielfältigung den IBM Corporation Copyrightvermerk enthalten muss. Weitere das Copyright betreffende Rechte werden nur nach vorheriger schriftlicher Zustimmung durch die IBM Corporation gewährt. Die Veröffentlichung dient nicht zu Produktionszwecken. IBM übernimmt keine Haftung. **Die in diesem Dokument aufgeführten Beispiele sollen lediglich der Veranschaulichung und keinem anderen Zweck dienen.**

Marken

IBM, das IBM Logo, Tivoli, das Tivoli-Logo, AIX, Cross-Site, NetView, OS/2, Planet Tivoli, RS/6000, Tivoli Certified, Tivoli Enterprise, Tivoli Enterprise Console, Tivoli Ready und TME sind in gewissen Ländern Marken oder eingetragene Marken der International Business Machines Corporation.

Microsoft, Windows, Windows NT und das Logo von Windows sind in gewissen Ländern Marken der Microsoft Corporation.

UNIX ist in gewissen Ländern eine eingetragene Marke und wird ausschließlich über X/Open Company Limited lizenziert.

Namen anderer Unternehmen, Produkte und Dienstleistungen können Marken oder Dienstleistungen anderer Unternehmen sein.

Bemerkungen

Hinweise auf Produkte, Programme oder Dienstleistungen von Tivoli Systems oder IBM in dieser Veröffentlichung bedeuten nicht, dass diese in allen Ländern, in denen Tivoli Systems oder IBM vertreten ist, angeboten werden. Hinweise auf diese Produkte, Programme oder Dienstleistungen bedeuten nicht, dass nur Produkte, Programme oder Dienstleistungen von Tivoli Systems oder IBM verwendet werden können. Im Rahmen der gültigen gewerblichen oder anderen Schutzrechte von Tivoli Systems oder IBM können äquivalente Produkte, Programme oder Dienstleistungen an Stelle der angegebenen Produkte, Programme oder Dienstleistungen verwendet werden. Die Verantwortung für den Betrieb in Verbindung mit Fremdprodukten liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich erwähnt sind. Für die in diesem Dokument beschriebenen Produkte und Verfahren kann es Patente oder Patentanmeldungen von Tivoli Systems oder IBM geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf Englisch formuliert werden.

Inhaltsverzeichnis

Vorwort xvii

Zielgruppe xvii

Inhalt dieses Handbuchs xvii

Veröffentlichungen xix

Erforderliche Referenzliteratur xix

Onlineveröffentlichungen xx

Veröffentlichungen bestellen xxi

Rückmeldungen zu Veröffentlichungen xxi

Kundenunterstützung anfordern xxi

In diesem Handbuch verwendete Konventionen xxii

In dieser Ergänzung verwendete Konventionen xxii

Symbole xxiii

Kapitel 1. Einführung in die Benutzer- und Gruppenverwaltung 1

Konzepte für plattformspezifische Benutzerverwaltung 3

UNIX-Plattformen 3

Benutzeranmeldung und Authentifizierung 3

Benutzer und Gruppen 4

Network Information System 5

Windows NT 5

Benutzerauthentifizierung 5

Local Security Authority 6

Security Account Manager 6

Security Reference Monitor 6

Benutzeranmeldung 7

Benutzer und Gruppen 8

Tivoli unter Windows NT verwenden 8

Windows 2000 9
Globale Kataloge. 9
Benutzerauthentifizierung 10
Local Security Authority 10
Active Directory 10
Sicherheitsbeschreibung. 10
Sicherheitskontext 11
Zugriffsüberprüfung. 11
Security Account Manager. 11
Benutzeranmeldung 12
Benutzer und Gruppen. 12
Tivoli unter Windows 2000 verwenden 13
Novell NetWare-Verzeichnisdienst 15
Objekte im NetWare-Verzeichnisdienst. 16
Benutzeranmeldung und Authentifizierung 16
Benutzer und Gruppen. 16
Tivoli unter NetWare verwenden 17
OS/390-Resource Access Control Facility 17
RACF-Datenbank 17
RACF-Segmente 18
Benutzerauthentifizierung 18
Ressourcenberechtigung. 19
RACF-Benutzerattribute. 19
RACF-Gruppen 20
Lightweight Directory Access Protocol (LDAP) 21
Funktionsweise der Benutzer- und Gruppenverwaltung. 22
Benutzer- und Gruppenprofile 23
Richtlinien für Benutzer- und Gruppenprofile. 24
Subskribenten einrichten 24

Daten an Profile weitergeben 25
Profile verteilen 26
Kennwortsteuerung 28
Benutzersuchfunktion 28
Dateisperren und Kollisionsvermeidung 29
Sicherheitsverwaltung 29
Task-spezifische Berechtigungsklassen 31
Berechtigungsklassen für Benutzerprofile 33
Berechtigungsklassen für Kennwortänderungen 33
Berechtigungsklassen für globale Attributänderungen 34
Berechtigungsklassen für Änderungen an Endpunktattributen 36
Große Anzahl Benutzer verwalten 38
Tausende Benutzer derselben Abteilung verwalten 38
Tausende Benutzer unterschiedlicher Abteilungen verwalten 40

Kapitel 2. Tivoli SecureWay User Administration installieren 43

Tivoli SecureWay User Administration - Installationspakete 44
Softwarevoraussetzungen 46
Hardwarevoraussetzungen 47
Anmerkungen vor der Softwareinstallation 47
Mit Tivoli Software Installation Service installieren 48
Tivoli SecureWay User Administration installieren 49
Arbeitsoberfläche 50
Befehlszeile 53
Tivoli SecureWay User Administration Gateway Package installieren 53
Arbeitsoberfläche 54
Befehlszeile 55

LDAP-Pakete installieren 56
Arbeitsoberfläche 56
Befehlszeile 58
OS/2-Pakete installieren 59
Arbeitsoberfläche 59
Befehlszeile 60
AS/400-Pakete installieren 61
Arbeitsoberfläche 62
Befehlszeile 64
OnePassword-Paket installieren 65
Arbeitsoberfläche 65
Befehlszeile 67
Befehl 'wonepassinst' ausführen 67
Zusätzliche Verwendungsmöglichkeiten von 'wonepassinst' 69
Befehl 'wpasswd' installieren 69
Tivoli SecureWay User Administration aktualisieren 70
Arbeitsoberfläche 70
Befehlszeile 71
Tivoli SecureWay User Administration-Pakete deinstallieren 72

Kapitel 3. Planung und Einsatz 75

Ihre Bedürfnisse hinsichtlich der Benutzerverwaltung feststellen 76
Personen, die auf Benutzerkonten zugreifen müssen 76
Funktionsbereiche 76
Berechtigungsklassen und Zuständigkeiten 77
Geschäftsanforderungen 80
Test 82

Kapitel 4. Kennwortverwaltung 83

Befehl 'wpasswd' verwenden. 84
Berechtigungsklassen für Kennwortänderungen 86
Kennwörter und Endpunktarten 87
Allgemeine und endpunktartspezifische Kennwörter 89
Nur das allgemeine Kennwort ändern. 90
Kennwortänderung durch Benutzer steuern. 91
Kennwortqualitätsregeln. 92
Unterstützte Security Manager-Kennwortrichtlinien 94
Nicht unterstützte Security Manager-Kennwortrichtlinien 99
Windows 2000-Kennwortrichtlinien 100
Durchsetzung durch den Server oder Durchsetzung durch den Endpunkt. 100
Meldung von Verstößen gegen Kennwortrichtlinien 101
Leistungsspektrum von wpasswd 101
Kennwörter ändern 102
Dienstprogrammfunktionen 104
Verwendung durch den Endbenutzer oder Verwendung durch den Administrator 106
Verwendung auf verwalteten Knoten oder Verwendung auf TMA-Endpunkten 106
Interne Informationen zum Befehl wpasswd 107
Gültigkeitsprüfung für alte Kennwörter 108
Verwendung der Option –L 109
Verwendung von Mdist 109
Lange Kennwörter 110
Synchronisation von Tivoli ACF durch Tivoli SecureWay User Administration 110
Bei Verwaltung des Endpunkts durch Tivoli SecureWay User Administration 111
Bei Verwaltung des NIS-Servers durch Tivoli SecureWay User Administration 112

OnePassword 112
Voraussetzungen für die Verwendung von OnePassword 113
Als Benutzer OnePassword verwenden 114
Als Administrator OnePassword verwenden 115

Kapitel 5. Benutzerprofile einrichten 119

Einführung 119
Benutzerprofile einrichten 122
Benutzerprofile als verwaltete Ressourcen zuordnen 122
Arbeitsoberfläche 122
Befehlszeile 123
Benutzerprofile erstellen 123
Arbeitsoberfläche 124
Befehlszeile 125
Benutzerprofile klonen 126
Arbeitsoberfläche 127
Befehlszeile 128
Benutzerprofile löschen 129
Arbeitsoberfläche 130
Befehlszeile 131
Mit Richtlinien für Benutzerprofile arbeiten 131
Standardwertegruppen definieren 132
Arbeitsoberfläche 132
Befehlszeile 135
Plattformspezifische Standardwertegruppen inaktivieren 137
Richtlinien für Gültigkeitsprüfung definieren 138
Arbeitsoberfläche 139
Befehlszeile 142
Benutzerprofile verwalten 144
Daten an Benutzerprofile weitergeben 144

Arbeitsoberfläche 149
Befehlszeile 151
Standardwerte für Verteilung festlegen 152

Kapitel 6. Benutzerdatensätze erstellen 155

Neue Datensätze für Benutzerkonten erstellen 156
Allgemeine Informationen zu Benutzerkonten 160
Informationen zur Benutzeridentifikation 160
Informationen zur Postadresse 161
Informationen zu Subskribenten 161
Arbeitsoberfläche 162
Befehlszeile 164
Informationen zur Sicherheitsgruppe 165
Arbeitsoberfläche 165
Befehlszeile 167
Informationen zur Sicherheitsrichtlinie 169
Arbeitsoberfläche 169
Befehlszeile 171
Informationen zu Windows NT-Benutzerkonten 172
Informationen zur Windows NT-Anmeldung 173
Informationen zur Windows NT-Anmeldezeit 174
Informationen zum Windows NT-Kennwort 175
Informationen zum Windows NT-Verzeichnis 176
Informationen zur Windows NT-Gruppenzugehörigkeit 177
Informationen zu Windows NT-Workstations 177
Informationen zum Windows NT-Fernzugriff 178
Informationen zu Windows 2000-Benutzerkonten 180
Windows 2000-Verzeichnis 181
Windows 2000-Gruppen 182
Windows 2000-Anmeldung 183

Windows 2000-Anmeldezeit. 184
Windows 2000-Kennwort. 185
Windows 2000-Fernzugriff. 186
Windows 2000-Webgruppe 188
Windows 2000 - Zusätzliche Identifikationsgruppe 189
Informationen zu NetWare-Benutzerkonten. 190
Informationen zur NetWare-Anmeldung 190
Informationen zur NetWare-Anmeldezeit 193
Informationen zum NetWare-Kennwort 194
Informationen zum NetWare-Verzeichnis 196
Informationen zur NetWare-Netzwerkadresse 197
Informationen zur NetWare-Gruppenzugehörigkeit 201
Informationen zur NetWare-Sicherheit 201
Informationen zu NetWare-E-Mail 202
Informationen zu NetWare-fremden E-Mail-Adressen 203
Informationen zu NetWare-Anmeldeskripts. 204
Informationen zur NetWare-Speicherplatzbeschränkung auf Datenträgern 207
Informationen zu NetWare-Workstations. 208
Dienst-Browser für NetWare-Verzeichnisse verwenden 209
Informationen zu UNIX-Benutzerkonten 210
Informationen zur UNIX-Anmeldung 210
Informationen zum UNIX-Kennwort 212
Informationen zum UNIX-Verzeichnis 213
Unterstützung für UNIX-Basisverzeichnisse 214
UNIX-Basisverzeichnisse erstellen 215
UNIX-E-Mail 220

Kapitel 7. Benutzerdatensätze verwalten 221

Allgemeine Vorgänge für Benutzerdatensätze 223

Benutzerdatensätze suchen 223
Voraussetzungen 224
Benutzer hinzufügen 224
Benutzer suchen 225
Benutzer editieren 228
Benutzer löschen 228
Benutzerdatensätze anzeigen 229
Arbeitsoberfläche 230
Befehlszeile 231
Benutzerdatensätze editieren 231
Arbeitsoberfläche 232
Befehlszeile 233
Benutzerdatensätze zusammenfügen 234
Benutzerdatensätze löschen 236
Arbeitsoberfläche 236
Befehlszeile 237
Benutzerdatensätze formatieren 237
Ausgabe des Befehls 'wusrdbrep' 238
Benutzerdatensätze aus Tivoli entfernen 241
Gruppenprofile an Subskribenten verteilen 241
Arbeitsoberfläche 243
Befehlszeile 248
Benutzerdatensätze verwalten 248
Benutzerdatensätze kopieren 249
Arbeitsoberfläche 250
Befehlszeile 251
Benutzerdatensätze verschieben 252
Arbeitsoberfläche 252
Befehlszeile 253
Informationen in Benutzerdatensätzen sperren und freigeben 254

Arbeitsoberfläche 254
Befehlszeile 255
Das Fenster ″Benutzerprofilmerkmale″ aktualisieren 256
Benutzerdatensätze mit der Tivoli-Datenbank synchronisieren 257
Arbeitsoberfläche 258
Befehlszeile 260
Benutzerdatensätze überprüfen 261
Benutzerdatensätze abrufen 262
Arbeitsoberfläche 263
Befehlszeile 265
Benutzerdatensätze suchen 266
Von einer Profilkopie in eine andere wechseln 268
Benutzerdatensätze sortieren 270
Benutzerdatensatzattribute sortieren 272

Kapitel 8. Gruppenprofile einrichten 275

Mit Gruppenprofilen arbeiten 275
Gruppenprofile als verwaltete Ressourcen zuordnen 276
Arbeitsoberfläche 276
Befehlszeile 277
Gruppenprofile erstellen 277
Arbeitsoberfläche 278
Befehlszeile 280
Gruppenprofile klonen 280
Arbeitsoberfläche 281
Befehlszeile 282
Gruppenprofile löschen 283
Arbeitsoberfläche 284
Befehlszeile 285
Mit Richtlinien von Gruppenprofilen arbeiten 285

Standardwertegruppen definieren 286
Arbeitsoberfläche 286
Befehlszeile 289
Richtlinie für Gültigkeitsprüfung definieren 291
Arbeitsoberfläche 291
Befehlszeile 294
Gruppenprofile verwalten 296
Daten an Gruppenprofile weitergeben 296
Arbeitsoberfläche 297
Befehlszeile 298
Standardwerte für Verteilung festlegen 299

Kapitel 9. Gruppendatensätze verwalten 303

Neue Datensätze für Gruppenkonten erstellen 304
Arbeitsoberfläche 304
Befehlszeile 307
Gruppenkontodatensätze editieren 307
Arbeitsoberfläche 308
Befehlszeile 309
Gruppenkontodatensatz löschen 311
Arbeitsoberfläche 311
Befehlszeile 312
Gruppenprofile an Subskribenten verteilen 313
Arbeitsoberfläche 314
Befehlszeile 318
Kopien von Gruppenprofilen aus einem anderen Profil abrufen 318
Arbeitsoberfläche 319
Befehlszeile 321
Profildatenbank mit Systemdateien synchronisieren 321

Arbeitsoberfläche 322
Befehlszeile 324
Datensätze anhand der Profilrichtlinie überprüfen 324
Arbeitsoberfläche 325
Befehlszeile 326
Gruppendatensatz suchen 326
Von einer Profilkopie in eine andere wechseln 329
Gruppendatensätze sortieren 330
Gruppendatensatzattribute sortieren 332

Kapitel 10. Prüfprotokollierung 335

Steuerkomponente für die Prüfprotokollierung aktivieren 336
Aktive Parameter ermitteln 338
Stoppen und mit geänderten Parametern erneut starten 339
Format des Prüfprotokolls 340
Protokollierte Operationen von Tivoli SecureWay User Administration 343

Kapitel 11. Tivoli SecureWay User Administration anpassen 345

Anpassungsstrategie 346
Kategorien der Benutzer- und Gruppenverwaltung 347
Unterkategorien der Benutzer- und Gruppenverwaltung 348
Anzeigen der Benutzer- und Gruppenverwaltung 349
Kategorien und Unterkategorien löschen 350
Beispiel einer Dialoganpassung 350
Einem Profil neue Attribute hinzufügen 351
Profildialog ändern 352

Kapitel 12. Weitere Themen 355

Produktgeschichte 356
CCMS-Komponenten und -Prozesse 357
Tivoli-Profile 358
Profilmanager-Subskribenten 359
Subskribenten auf Datensatzebene 361
Profilverteilung 361
CCMS und AEF (Application Extension Facility) 363
CCMS-Verteilungsverarbeitung und AEF-Aktionen 364
Sonderverarbeitung für Kennwörter bei der Verteilung 365
Steuerung der Änderung von Oneshot-Attributen auf Basis des Endpunkt-Status 366
Oneshot-Attribute anzeigen 368
Der Einfluss von Verteilungsoptionen auf Benutzerkonten und Kennwörter 370
Benutzer- und Gruppen-Indexdatenbanken und der Befehl wchkadmdb 374
Der Standardwertegruppendatensatz und die Befehle waddprop, waddusrprop, wgenusrdef 378
Weitere Veröffentlichungen 379

Anhang A. AS/400-Benutzer verwalten 381

Vorteile einer Verwaltung von AS/400-Benutzerkonten über Tivoli 381
User Administration for AS/400 verwenden 382
Mit AS/400-Attributen und -Endpunkten arbeiten 383
AS/400-spezifische Funktionen 383
Weitergeben/Suchen 384
Verteilen/Aktualisieren 384
Kennwörter 384
Sonderfunktionen für AS/400 385
AS/400-spezifische Benutzerinformationen 386

OS/400-Benutzerkonten ändern 400

Anhang B. OS/2-Benutzer verwalten 403

Vorteile einer Verwaltung von OS/2-Benutzerkonten über Tivoli 403

Mit OS/2-Attributen und -Endpunkten arbeiten. 404

OS/2-Benutzerattribute im Tivoli-Benutzerprofil 405

OS/2-Konto 405

Optionen für OS/2-Konto. 409

Zuordnungen bei OS/2-Anmeldung 411

Allgemeine OS/2-Anwendungen 413

OS/2-Gruppenzugehörigkeit 414

Anmelde-Workstations 416

Funktionsweise von SecureWay User Administration auf OS/2-Endpunkten 417

OS/2-Endpunkt als primärer bzw. Backup-Domänencontroller 417

Verteilung an andere OS/2-Server und -Systeme. 418

Benutzer ohne Kennwort 418

Benutzer mit geändertem Kennwort 419

Benutzer mit geänderter Benutzer-ID (Anmeldename) 419

Benutzer in der OS/2-Gruppe 'SERVERS' 419

OS/2-Attributnamen in Benutzerprofilen. 420

OS/2-Ergebniscodes. 426

OS/2-Verteilungsfehler. 440

Glossar 443

Index 459

Vorwort

Das Handbuch *Tivoli SecureWay User Administration Management Handbuch* bietet Ihnen Task-orientierte Informationen zur Verwaltung von Benutzer- und Gruppenkonten mit Tivoli-Profilen. Das Handbuch enthält Hintergrundinformationen zu Benutzer- und Gruppenkonten, Informationen zur Verwaltung dieser Kontoarten durch Tivoli, Beispiele zur Einrichtung und Verwendung von Tivoli SecureWay User Administration für die Benutzer- und Gruppenverwaltung sowie Verfahren zur Verwendung aller Komponenten der Benutzerschnittstelle, einschließlich der grafischen Benutzerschnittstelle (GUI) und der Befehlszeilenschnittstelle (CLI).

Zielgruppe

Dieses Handbuch wendet sich an Systemadministratoren, die Tivoli SecureWay User Administration zur Einrichtung von Benutzer- und Gruppenkonfigurationsprofilen verwenden und mit Tivoli alltägliche Verwaltungs-Tasks für Benutzer- und Gruppenkonten ausführen.

Die Benutzer dieses Handbuchs sollten vertraut sein mit:

- Den Betriebssystemen Microsoft® Windows NT® und Windows 2000®
- Novell® NetWare®
- UNIX®
- Der Shell-Programmierung

Inhalt dieses Handbuchs

Dieses Handbuch besteht aus den folgenden Kapiteln:

- Einführung in die Benutzer- und Gruppenverwaltung

  Beschreibt die Benutzer- und Gruppenverwaltungsfunktionen und zeigt, welche Benutzer- und Gruppenkontoinformationen verwaltet werden. Außerdem enthält es realistische Szenarios für die Verwendung der Anwendung.

- Tivoli SecureWay User Administration installieren

  Beschreibt die Installation und Deinstallation von Tivoli SecureWay User Administration.

- Planung und Einsatz

  Enthält Informationen zum Planen, Testen und Einsetzen einer Tivoli SecureWay User Administration-Implementierung.

- Kennwortverwaltung

  Beschreibt die Kennwortverwaltung in Tivoli SecureWay User Administration.

- Benutzerprofile einrichten

  Beschreibt die Erstellung von Benutzerprofilen, die Einstellung der Standardwertegruppe und der Richtlinie für die Gültigkeitsprüfung sowie die Weitergabe von Daten an Benutzerprofile.

- Benutzerdatensätze erstellen

  Beschreibt das Erstellen von Benutzerdatensätzen, darunter das Hinzufügen allgemeiner Informationen sowie Windows NT-, NetWare- und UNIX-Benutzerinformationen zu einem Profil.

- Benutzerdatensätze verwalten

  Beschreibt die Ausführung allgemeiner Tasks im Zusammenhang mit Benutzerdatensätzen, wie beispielsweise die Suche nach Datensätzen und deren Bearbeitung.

- Gruppenprofile einrichten

  Beschreibt die Erstellung von Gruppenprofilen, die Einstellung der Standardwertegruppe und der Richtlinie für die Gültigkeitsprüfung sowie die Weitergabe von Daten an Gruppenprofile.

- Gruppendatensätze verwalten

  Beschreibt die Erstellung von Gruppendatensätzen sowie die Ausführung allgemeiner Tasks im Zusammenhang mit diesen Datensätzen, wie beispielsweise deren Bearbeitung und Überprüfung auf ihre Gültigkeit anhand der entsprechenden Richtlinie.

- Prüfprotokollierung

  Beschreibt die Verwendung der Prüfprotokollsteuerkomponente.

- Tivoli SecureWay User Administration anpassen

  Beschreibt die Anpassung von Tivoli SecureWay User Administration unter Verwendung von Tivoli AEF (Application Extension Facility).

- Weitere Themen

  Beschreibt die Verteilung von Benutzerprofilen, die Sonderverarbeitung von Kennwörtern, die Speicherung von Benutzerdaten und Indexierungsmethoden sowie andere Themen.

- AS/400-Benutzer verwalten

  Beschreibt die Verwendung von Tivoli SecureWay User Administration in einer AS/400-Umgebung.

- OS/2-Benutzer verwalten

  Beschreibt die Verwendung von Tivoli SecureWay User Administration in einer OS/2-Umgebung.

Veröffentlichungen

In diesem Kapitel wird die erforderliche Referenzliteratur aufgeführt. Außerdem werden der Onlinezugriff auf die Tivoli-Veröffentlichungen sowie deren Bestellung beschrieben. Außerdem erfahren Sie, auf welche Weise Sie Anmerkungen zu den Tivoli-Veröffentlichungen abgeben können.

Erforderliche Referenzliteratur

Bevor Sie die in diesem Handbuch beschriebene Software installieren und verwenden, müssen Sie mit den Inhalten der dazugehörigen Dokumentation vertraut sein.

- *Tivoli Management Framework: Einsatzplanung*

  Erläutert die Planung für das Einsetzen einer Tivoli-Umgebung. Außerdem werden die Komponente Tivoli Management Framework und dessen Dienste beschrieben.

- *Tivoli Enterprise Installation Guide*

  Erläutert Installation und Aktualisierung von Tivoli Enterprise-Software innerhalb der Tivoli Management Region (TMR) unter Verwendung der von Tivoli Software Installation Service und

Tivoli Management Framework zur Verfügung gestellten Installationsmechanismen. Zur Tivoli Enterprise-Software gehören der TMR-Server, verwaltete Knoten, Gateways, Endpunkte und RIM-Objekte (RIM = RDBMS Interface Module). Dieses Handbuch enthält außerdem Informationen zum Lösen von Installationsproblemen.

- *Tivoli Management Framework Benutzerhandbuch*

  Enthält eine Beschreibung der den Tivoli Management Framework-Diensten zugrundeliegenden Konzepte sowie Informationen zur Verwendung dieser Dienste. Es enthält Anweisungen zur Ausführung von Tasks über die Tivoli-Arbeitsoberfläche und über die Befehlszeile.

- *Tivoli Management Framework Reference Manual*

  Enthält ausführliche Informationen zu den CLI-Befehlen von Tivoli Management Framework. Dieses Handbuch ist auch beim Schreiben von Skripts hilfreich, die später als Tivoli-Tasks ausgeführt werden sollen. Es dokumentiert außerdem die in Tivoli enthaltenen Richtlinienskripts.

- *Tivoli Management Framework Release Notes*

  Enthält wichtige Informationen über das Tivoli Management Framework-Release.

Onlineveröffentlichungen

Über die Tivoli-Website für Kundenunterstützung können Sie auf eine Vielzahl von Tivoli-Veröffentlichungen zugreifen:

http://www.tivoli.com/support/documents/

Sie stehen im PDF- und/oder HTML-Format zur Verfügung. Ein Teil dieser Dokumentation liegt in mehreren Sprachen vor.

Für den Zugriff auf den Großteil der Dokumentation benötigen Sie eine ID und ein Kennwort. Diese können Sie bei Bedarf auf folgender Website anfordern:

http://www.tivoli.com/support/getting/

Veröffentlichungen bestellen

Zusätzliche Exemplare können Sie per E-Mail bestellen:

LITERATA@DE.IBM.COM

Die Bestellung kann auch per Telefon oder Fax erfolgen.

- Telefon: 0049-180-55090 bzw. 0180-55090
- Fax: 07032-15-3300
- Die in anderen Ländern gültigen Telefonnummern finden Sie auf folgender Website:
  http://www.tivoli.com/inside/store/lit_order.html

Rückmeldungen zu Veröffentlichungen

Ihre Erfahrungen mit Tivoli-Produkten und -Dokumentationen sind für uns von besonderer Bedeutung. Auch sind wir sehr an Ihren Kommentaren und Verbesserungsvorschlägen interessiert, die Sie uns auf einem der folgenden Wege mitteilen können:

- Senden Sie eine E-Mail an pubs@tivoli.com. (Bitte formulieren Sie Ihre E-Mail in englischer Sprache.)
- Füllen Sie das Formular für Kundenrückmeldung auf folgender Website aus: http://www.tivoli.com/support/survey/

Kundenunterstützung anfordern

Sollte sich ein Problem in Zusammenhang mit einem Tivoli-Produkt ergeben, können Sie die Tivoli-Kundenunterstützung kontaktieren. Informationen hierzu finden Sie im *Tivoli Customer Support Handbook* auf der folgenden Website (nur in Englisch verfügbar):

http://wwwtivoli.com/support/handbook/

Dieses Buch enthält neben Informationen zur Kontaktaufnahme mit der Tivoli-Kundenunterstützung je nach Dringlichkeit des Problems auch folgende Informationen):

- Registrierung und Anspruch
- Telefonnummern und E-Mail-Adressen der jeweiligen Länder
- Informationen, die Sie beim Kontaktieren der Kundenunterstützung bereit halten sollten

In diesem Handbuch verwendete Konventionen

In dieser Ergänzung werden neben bestimmten Symbolen verschiedene Schriftbildkonventionen für bestimmte Begriffe und Aktionen verwendet.

In dieser Ergänzung verwendete Konventionen

In dieser Ergänzung werden folgende Schriftbildkonventionen verwendet:

Fett Befehle, Schlüsselwörter, Dateinamen, Berechtigungsklassen, URLs und andere Informationen, die Sie, wie in der Anleitung angegeben, eingeben müssen, sind **fett** gedruckt.

Fenster- und Dialognamen sowie andere Steuerelemente werden ebenfalls **fett** dargestellt.

Kursiv Vom Benutzer einzugebende Variablen und Werte sind *kursiv* gedruckt.

Hervorhebungen von Wörtern und Ausdrücken im Text sind ebenfalls *kursiv*.

`Monospace-Schrift`
Beispiele für Codes, Ausgaben und Systemnachrichten werden in `Monospace-Schrift` dargestellt.

Symbole

Die folgenden Symbole stellen die Benutzer- und Gruppenprofilressourcen dar:

Benutzer- und Gruppenprofilressourcen werden in der Umgebung eines Profilmanagers erstellt. Nach der ersten Verteilung eines Benutzer- oder Gruppenprofils wird das Profilsymbol im Dialog der Subskribenten dargestellt. Bei diesen Subskribenten kann es sich um Windows NT-Domänenserver, Windows 2000-Serverendpunkte, Novell NetWare-NDS-Serverendpunkte, UNIX-verwaltete Knoten und -Endpunkte, NIS-Domänen und andere verwaltete Knoten bzw. andere Profilmanager handeln. Das Symbol der Benutzersuchfunktion befindet sich auf der Tivoli-Arbeitsoberfläche. Mit dem Dialog **Benutzersuchfunktion** können Sie einen Benutzer schnell lokalisieren.

1

Einführung in die Benutzer- und Gruppenverwaltung

Systemadministratoren müssen unter Umständen viel Zeit für die Verwaltung von Benutzerkonten und Zugehörigkeiten in einem großen Unternehmen aufwenden. Im Unternehmen werden ständig Benutzerkonten hinzugefügt und entfernt. Außerdem müssen Benutzerkonten regelmäßig aktualisiert werden, wenn sich die Anforderungen der Benutzer ändern.

Früher mussten Systemadministratoren mit Benutzerkonten in Umgebungen mit nur einem Betriebssystem arbeiten, z. B. einer UNIX-Umgebung oder Großrechnerumgebung. Heute gibt es in den meisten großen Unternehmen Benutzer, die Konten in Umgebungen mit verschiedenen Betriebssystemen benötigen, wie beispielsweise UNIX, Windows 2000, Windows NT, NetWare, OS/2, OS/390 oder OS/400.

Die Betriebssysteme UNIX, Windows NT, Windows 2000 und NetWare verfügen über eigene Konfigurationsdateien oder Datenbanken, die die Benutzerkonten für das jeweilige System definieren. Darüber hinaus verfügen die verschiedenen UNIX-Systeme über eigene Konfigurationsdateien für Benutzerkonten. Unter Windows NT gibt es zudem globale und lokale Konten.

Zusätzlich zu den Unterschieden zwischen den Benutzerkonten der Umgebungen mit verschiedenen Betriebssystemen gibt es zwischen den Systemen und Bereichen eines Unternehmens unvermeidbare Unterschiede in der Benutzerkontenverwaltung.

Tivoli SecureWay User Administration stellt Ihnen die erforderlichen Tools für die Verwaltung von Benutzerkonten auf den gängigen Betriebssystemen Windows NT, Windows 2000, NetWare, OS/2, OS/4, OS/390 und den wichtigsten UNIX-Plattformen (AIX, HP-UX, Solaris und Linux) zur Verfügung. Tivoli SecureWay User Administration enthält folgende Benutzer- und Gruppenverwaltungsfunktionen:

- Eine grafische Benutzerschnittstelle (GUI) zur zentralen Verwaltung von Benutzerkonten unter UNIX, Windows, NetWare und anderen Plattformen
- Schablonen, mit denen Sie durch Eingabe weniger Daten einen vollständigen Datensatz erstellen können
- Tools zum schnellen Suchen, Bearbeiten, Erstellen und Löschen eines bestimmten Benutzerdatensatzes
- Zentrale Administratorsteuerung von Konten in Kombination mit begrenzter Benutzereingabesteuerung
- Task-spezifische Berechtigungsklassen, über die ein leitender Systemadministrator den verschiedenen Informationen in den Benutzerkonten unterschiedliche Zugriffsebenen zuordnen kann
- Verwaltung von allgemeinen Benutzerinformationen sowie von Kontoinformationen unter UNIX, Windows und NetWare und anderen Plattformarten in einem Benutzerdatensatz
- Echte Client-/Serverunterstützung

In diesem Kapitel werden folgende Benutzer- und Gruppenverwaltungsfunktionen beschrieben:

- Konzepte für plattformspezifische Benutzerverwaltung
- Funktionsweise der Benutzer- und Gruppenverwaltung
- Komponenten für die Benutzerkonten- und Gruppenverwaltung
- Benutzer- und Gruppenprofile
- Richtlinien für Benutzer- und Gruppenprofile
- Kennwortsteuerung

- Benutzersuchfunktion
- Datensätze sperren
- Sicherheitsverwaltung
- Beispiele für die Verwaltung vieler Benutzer

Konzepte für plattformspezifische Benutzerverwaltung

Die Benutzerverwaltung auf Plattformebene (Betriebssystemebene) beinhaltet die Authentifizierung des Benutzerzugriffs auf Systemressourcen und die Sicherheitsverwaltung von Benutzerkontoinformationen. Auf den verschiedenen Plattformen wird die Benutzerkonten- und Sicherheitsverwaltung unterschiedlich gehandhabt. Mit Tivoli SecureWay User Administration können Sie Benutzerkonten plattformübergreifend verwalten, ohne Änderungen an den jeweiligen plattformspezifischen Funktionen vornehmen zu müssen. Die folgenden Abschnitte enthalten eine Übersicht dazu, wie auf den einzelnen Plattformen die Benutzerverwaltung gehandhabt wird.

UNIX-Plattformen

Die folgenden Abschnitte enthalten allgemeine Informationen zur Benutzerverwaltung auf UNIX-Plattformen. Obwohl sich die UNIX-Plattformen im Allgemeinen ähneln, gibt es dennoch einige Unterschiede. Es ist möglich, dass sich die Systemdateinamen von UNIX-Plattform zu UNIX-Plattform unterscheiden.

Anmerkung: In den nachfolgenden Abschnitten werden die Namen der Systemdateien unter AIX verwendet.

Benutzeranmeldung und Authentifizierung

Benutzer melden sich durch Eingabe einer gültigen Benutzer-ID und eines Kennworts an UNIX-Systemen an. Auf UNIX-Systemen wird das Kennwort verschlüsselt und niemals als lesbarer Text angezeigt. Die Benutzer-ID wird mit den Einträgen in der Datei **/etc/passwd** und das Kennwort mit den Einträgen in der Datei **/etc/security/passwd** auf dem lokalen System verglichen.

Anmerkung: Unter UNIX ist auch eine Authentifizierung von fernen Datenbanken wie beispielsweise NIS möglich.

Sobald ein Benutzer authentifiziert wurde und ihm eine Anmeldesitzung gewährt wurde, wird die Benutzerumgebung vom System erstellt. Das System erstellt zuerst eine globale Umgebung und dann eine benutzerspezifische Umgebung. Die globale Umgebung wird normalerweise über die Dateien **/etc/profile** und /etc/environment erstellt, wobei es sich um systemweite Dateien handelt. Über diese Dateien werden die Umgebungsvariablen für die meisten Systembenutzer festgesetzt. Sie werden auch dazu verwendet, schreibgeschützte Umgebungsvariablen festzulegen, die vom Benutzer weder geändert noch entfernt werden können.

Eine benutzerspezifische Umgebung wird über die Benutzerdatei **.profile** und andere Dateien, die sich üblicherweise im Basisverzeichnis des Benutzers befinden, erstellt.

Innerhalb eines UNIX-Systems wird ein Benutzer durch eine eindeutige numerische Benutzer-ID (UID) sowie durch eine primäre Gruppen-ID (GID) identifiziert. Die Benutzer-ID bzw. Gruppen-ID kann vom Systemadministrator geändert werden.

Meldet sich ein Benutzer mit seinem Anmeldenamen an (der in der Regel vom tatsächlichen Namen abgeleitet wurde), verfolgt das System gemäß der numerischen Benutzer-ID alle Besitz- und Zugriffsrechte. Mit der Datei **/etc/passwd** wird der Anmeldename in die Benutzer-ID umgesetzt.

Tivoli SecureWay User Administration ermöglicht die Verwaltung von Benutzerinformationen, die in den verschiedenen UNIX-Systemdateien enthalten sind. Eine Liste der betreffenden Dateien sowie der Namen auf den unterschiedlichen UNIX-Plattformen finden Sie im Handbuch *Tivoli SecureWay User Administration Reference Manual.*

Benutzer und Gruppen

Jeder Benutzer im System gehört mindestens einer Gruppe an. Die einzelnen Gruppen setzen sich aus Benutzern zusammen, die über ähnliche Zugriffsrechte und Berechtigungen verfügen. Einer

Benutzergruppe kann mit Hilfe der Gruppenberechtigung der Zugriff auf bestimmte Dateien oder Verzeichnisse auf einfache Weise eingeräumt werden. Die meisten Benutzer gehören normalerweise der Standardgruppe *staff* (Personal) an. Systemadministratoren können Gruppen erstellen und diesen Benutzer zuordnen. Ein einzelner Benutzer kann mehreren Gruppen gleichzeitig angehören.

In allen UNIX-Systemen gibt es Standardsystemgruppen und -benutzer, die bei der Installation des Systems definiert werden. Informationen zu UNIX-Benutzer- und -Gruppenkonten, die von Tivoli SecureWay User Administration unterstützt werden, finden Sie im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Network Information System

Network Information Service (NIS) ist ein UNIX-Dienst zur Verwaltung einer großen Anzahl von Systemen. NIS stellt dabei aktuelle Informationen aus den zentralen UNIX-Dateien für die Benutzer-, System- und Netzwerkverwaltung zur Verfügung. NIS wird in den meisten Fällen für die Gewährleistung der Konsistenz von Benutzernamen und -IDs, Gruppennamen und -IDs sowie Kennwörtern auf verschiedenen Systemen verwendet. NIS nimmt dabei keine Verteilung der eigentlichen Dateien mit diesen Daten vor. Stattdessen werden die Informationen von den Dateien zur Erstellung einer NIS-Liste verwendet. Hierbei handelt es sich um eine von den NIS-Clients erstellte Datenbankdatei, auf die diese auch zugreifen.

Sie können mit Tivoli SecureWay User Administration Benutzerkonten innerhalb einer NIS-Domäne verwalten. Weitere Informationen hierzu finden Sie im Handbuch *Tivoli User Administration NIS Management Guide*.

Windows NT

Die nachfolgenden Abschnitte enthalten eine allgemeine Übersicht über die Benutzerverwaltung unter Windows NT.

Benutzerauthentifizierung

Windows NT verfügt über verschiedene Sicherheitseinrichtungen, mit denen der Zugriff auf Dateien, Verzeichnisse und andere Systemressourcen gesteuert wird.

Dazu gehören folgende Einrichtungen:

- Local Security Authority
- Security Account Manager
- Security Reference Monitor

Local Security Authority

Die Local Security Authority (LSA) stellt sicher, dass der Benutzer über die erforderlichen Berechtigungen verfügt, um auf das System zuzugreifen. Diese Funktion erstellt Zugriffs-Token während des Anmeldevorgangs, verwaltet die Sicherheitsrichtlinien, definiert die Überwachungsrichtlinien und schreibt Überwachungsnachrichten in das Ereignisprotokoll.

Security Account Manager

Der Security Account Manager (SAM) ist für die Pflege einer Datenbank mit Informationen über die Benutzer- und Gruppenkonten verantwortlich. SAM stellt Gültigkeitsprüfungsdienste für LSA bereit und vergleicht die vom Benutzer während der Anmeldung eingegebenen Daten mit den Informationen in der Datenbank.

SAM stellt beim Erstellen eines Benutzerkontos eine Sicherheits-ID (SID) für den Benutzer und die SID der Gruppen zur Verfügung, denen der Benutzer angehört. Bei der SID handelt es sich um eine vom System generierte, aus 32 Bit bestehende Zahlenfolge, mit der jedes Konto innerhalb des Systems (bzw. der Domäne) eindeutig identifiziert wird. Diese ID entspricht der numerischen UNIX-Benutzer-ID (UID), anders als unter UNIX kann der Systemadministrator die SID jedoch nicht ändern.

Security Reference Monitor

Der Security Reference Monitor (SRM) überprüft den Zugriff auf Objekte und Ressourcen (z. B. Dateien, Verzeichnisse, Drucker usw.). Er schützt dabei alle Ressourcen vor unbefugten Zugriffen oder Änderungen und generiert die entsprechenden Überwachungsnachrichten. Ein direkter Ressourcenzugriff durch Benutzer ist in Windows NT nicht möglich. Benutzeranforderungen für den Zugriff auf eine Ressource müssen von SRM überprüft werden.

Benutzeranmeldung

Der Benutzer muss zum Anmelden am System die Tastenkombination **Strg+Alt+Entf** drücken, um das Dialogfenster **Anmeldeinformationen** anzuzeigen. Hier muss er einen Benutzernamen und ein Kennwort eingeben und sich entscheiden, ob er sich am lokalen Computer oder an der Domäne anmelden möchte.

Das System überprüft daraufhin in der SAM-Datenbank, ob der Benutzer vorhanden ist und ob ein gültiges Kennwort eingegeben wurde. Verfügt der Benutzer über ein Konto und hat er ein gültiges Kennwort eingegeben, erstellt das Sicherheitssubsystem ein *Zugriffs-Token*. Mit diesem Token wird der Benutzer identifiziert. Es enthält Informationen wie die Sicherheits-ID des Benutzers, den Benutzernamen sowie die Gruppen, denen der Benutzer angehört.

Dieses Zugriffs-Token (bzw. eine Kopie) wird jedem vom Benutzer gestarteten Prozess zugeordnet. Die Kombination aus Zugriffs-Token und Prozesszuordnung wird als *Subjekt* bezeichnet. Beim Zugriff auf eine Ressource (Datei, Verzeichnis usw.) wird der Inhalt des Subjekts anhand der Zugriffssteuerungsliste (Access Control List, ACL) des Objekts, auf das der Zugriff erfolgt, durch eine Routine für die Gültigkeitsprüfung des Zugriffs überprüft.

Die Umgebungsinformationen des Benutzers werden in einem Profil gespeichert. Dieses Profil wird bei jeder Anmeldung des Benutzers geladen. Es gibt verschiedene Profilarten. Das *persönliche* Benutzerprofil kann vom Benutzer geändert werden. Alle Änderungen, die der Benutzer an der Umgebung vornimmt, werden beim Abmelden des Benutzers in diesem Profil gespeichert.

Das *verbindliche* Benutzerprofil (Mandatory Profile) kann vom Systemadministrator für die Benutzer innerhalb einer Domäne festgelegt werden. In diesem Profil werden die Umgebungseinstellungen definiert, die bei der Benutzeranmeldung verwendet werden. Es definiert außerdem, welche Anwendungen nach der Anmeldung gestartet bzw. welche Netzwerklaufwerke verbunden werden. Nimmt ein Benutzer Änderungen an diesen Umgebungseinstellungen vor, werden diese beim Abmelden nicht gespeichert.

Benutzer und Gruppen

Alle Benutzer in Windows NT werden mindestens einer Gruppe zugeordnet. Wie auch auf den UNIX-Plattformen erleichtert das Zusammenfassen von Benutzern in Gruppen die Benutzerverwaltung, da der Administrator die Zugriffsberechtigungssteuerung auf Gruppenebene vornehmen kann.

Windows NT unterstützt drei Kontoarten:

- Benutzerkonten
- Lokale Gruppen
- Globale Gruppen

Auf jeder Maschine können lokale Gruppen definiert werden. Lokale Gruppen beziehen sich dabei nur auf diese Maschine, d. h., die in diesen lokalen Gruppen definierten Berechtigungen gelten ausschließlich für lokale Ressourcen. Unter Windows NT stehen auf jeder Maschine standardmäßig vordefinierte lokale Gruppen zur Verfügung.

Bei einer Standalone-Maschine können nur lokale Benutzerkonten einer lokalen Benutzergruppe angehören. Gehört die Maschine einer Domäne an, kann die lokale Gruppe sowohl lokale Benutzerkonten als auch Domänenbenutzerkonten, Benutzerkonten vertrauter Domänen und globale Gruppen der Domäne bzw. einer vertrauten Domäne enthalten.

Globale Gruppen werden auf Domänenebene definiert und können an ferne Domänen exportiert werden. Mitglieder von globalen Gruppen können Domänenbenutzerkonten oder Benutzerkonten vertrauter Domänen sein. Ein lokaler Benutzer hingegen kann einer globalen Gruppe nicht angehören. Windows NT verfügt standardmäßig über mehrere integrierte globale Gruppenkonten.

Tivoli unter Windows NT verwenden

Wenn Tivoli SecureWay User Administration auf einem Windows NT-Domänenserver installiert ist, verwaltet die Anwendung die Domänenkonten, die Domänengruppenzugehörigkeiten und die lokalen Gruppenzugehörigkeiten auf dem Server. Wenn Tivoli SecureWay

User Administration auf einer NT-Workstation installiert ist, verwaltet die Anwendung lokale Workstation-Konten und lokale Gruppenzugehörigkeiten auf dieser Maschine. Tivoli SecureWay User Administration wird normalerweise auf den Domänenservern installiert und nicht auf den einzelnen Workstations.

Windows 2000

Die folgenden Abschnitte enthalten allgemeine Informationen zur Benutzerverwaltung unter Windows 2000.

Globale Kataloge

Für die Tivoli SecureWay User Administration-Unterstützung des Windows 2000-Endpunkts ist der Einsatz eines Servers für globale Kataloge erforderlich. Globale Kataloge sind konfigurierbar und können selektiv auf jedem beliebigen Windows 2000-Server aktiviert werden. Wenn ein Windows 2000-Endpunkt die Zieladresse für Tivoli SecureWay User Administration ist und sich in einer Domäne befindet, die nicht über einen globalen Katalog verfügt, können Operationen nicht erfolgreich ausgeführt werden.

Im globalen Katalog sind alle Objekte aller Domänen im Windows 2000-Verzeichnis sowie eine Teilmenge der Merkmale jedes einzelnen Objekts enthalten. Der Globale Katalog kann also als Repository verwendet werden und hat dieselben Funktionen wie ein globales Adressbuch. Der Windows 2000-Endpunkt verwendet den globalen Katalog zur schnellen Suche nach und zur Bearbeitung von Benutzerinformationen.

Weitere Informationen zu globalen Katalogen finden Sie in den Windows 2000-Installations- und Konfigurationsdokumentationen oder auf den folgenden Websites von Microsoft:

- MSDN Online unter der Adresse **http://msdn.microsoft.com/default.asp**
- Windows 2000 Developer Center unter der Adresse **http://msdn.microsoft.com/windows 2000**

Benutzerauthentifizierung

Windows 2000 verfügt über verschiedene Sicherheitseinrichtungen zur Steuerung des Zugriffs auf Dateien, Verzeichnisse und andere Systemressourcen. Dazu gehören folgende Einrichtungen:

- Local Security Authority (Lokale Sicherheitsautorität)
- Active Directory
- Sicherheitsbeschreibung
- Sicherheitskontext
- Zugriffsüberprüfung
- Security Account Manager (Sicherheitskontenverwaltung)

Local Security Authority

Die Local Security Authority (LSA) stellt sicher, dass der Benutzer über die erforderlichen Berechtigungen verfügt, um auf das System zuzugreifen. Diese Funktion erstellt Zugriffs-Token während des Anmeldevorgangs, verwaltet die Sicherheitsrichtlinien, definiert die Überwachungsrichtlinien und schreibt Überwachungsnachrichten in das Ereignisprotokoll.

Active Directory

Tivoli SecureWay User Administration verwendet Windows 2000 Active Directory zur Speicherung von notwendigen Benutzerinformationen einschließlich der Authentifizierungsdaten und Kennwörter.

Mit Hilfe von Active Directory können Administratoren bestimmte Verwaltungsberechtigungen und Tasks an einzelne Benutzer und Gruppen delegieren. Das Zurücksetzen von Benutzerkennwörtern kann beispielsweise an Betriebsadministratoren delegiert werden. Verantwortungsvollere Aufgaben wie das Erstellen von Benutzern können IT-Administratoren vorbehalten werden.

Sicherheitsbeschreibung

Jedes Verzeichnisobjekt verfügt über eine eigene Sicherheitsbeschreibung, die Sicherheitsinformationen zum Schutz des Objekts enthält. Jeder Sicherheitsbeschreibung kann unter anderem eine

benutzerdefinierte Zugriffssteuerungsliste (DACL) zugeordnet werden. Eine DACL enthält eine Liste mit Zugriffssteuerungseinträgen (ACEs). Jeder ACE erteilt oder verweigert einem Benutzer bzw. einer Gruppe Zugriffsberechtigungen. Die Zugriffsberechtigungen entsprechen den Operationen, z. B. das Lesen und Schreiben von Merkmalen, die für das Objekt ausgeführt werden können.

Sicherheitskontext

Wenn Sie auf ein Verzeichnisobjekt zugreifen, gibt Ihre Anwendung die Berechtigungen des Sicherheits-Principals an, der versucht, auf das Objekt zuzugreifen. Sobald diese Berechtigungen authentifiziert wurden, bestimmen sie den Sicherheitskontext Ihrer Anwendung, der die Gruppenzugehörigkeiten und Berechtigungen beinhaltet, die dem Sicherheits-Principal zugeordnet sind. Weitere Informationen zum Sicherheitskontext finden Sie in den vorherigen Abschnitten “Active Directory” und “Sicherheitsbeschreibung” oder im Abschnitt “Sicherheitskontext” in der MSDN-Dokumentation von Microsoft.

Zugriffsüberprüfung

Das System ermöglicht den Zugriff auf ein Objekt nur dann, wenn die Sicherheitsbeschreibung des Objekts dem Sicherheits-Principal, der versucht, die Operation auszuführen (bzw. den Gruppen, denen der Sicherheits-Principal angehört) die notwendigen Zugriffsberechtigungen erteilt.

Security Account Manager

In einem Multitasking-Betriebssystem wie beispielsweise Windows 2000 wird eine Vielzahl von Systemressourcen einschließlich Hauptspeicher, I/O-Einheiten, Dateien und Systemprozessoren des Computers von den Anwendungen gemeinsam benutzt. Windows 2000 unterstützt auch eine Systemrichtliniendatenbank, falls diese Unterstützung aktiviert ist.

Unabhängig davon, ob Systemrichtlinien den Zugriff über SAM-Konten ermöglichen, ist für Tivoli SecureWay User Administration und Windows 2000 Active Directory ein SAM-Kontoname für jeden Benutzer erforderlich. Weitere Informationen hierzu finden Sie im Abschnitt “Security Access Manager” in der MSDN-Dokumentation von Microsoft.

Benutzeranmeldung

Wenn sich Benutzer am System anmelden, müssen sie die Tastenkombination **Strg**+**Alt**+**Entf** verwenden, um den Dialog **Anmeldeinformationen** anzuzeigen. Der Benutzer muss dann einen Benutzernamen und ein Kennwort eingeben und entscheiden, ob er sich lokal oder an der Domäne anmelden möchte.

Das System überprüft zunächst im globalen Katalog bzw. in der Active Directory-Datenbank (wenn der globale Katalog nicht aktiv ist), ob der Benutzer vorhanden ist und ob ein gültiges Kennwort eingegeben wurde.

Benutzer können für die Anmeldung einen der drei folgenden Namen verwenden:

- Den normalen Verzeichnisnamen (bzw. *allgemeinen Namen*). Dies ist der allgemeine Name, der für ein Windows 2000-Konto verwendet wird
- Den SAM-Kontonamen. Dies ist ein eindeutiger Anmeldename, der zur Unterstützung von Clients und Servern aus Betriebssystemen vor Windows 2000 verwendet wird (wenn die Richtlinien Anmeldungen von Systemen vor Windows 2000 ermöglichen)
- Den Namen des Benutzer-Principals (bzw. *Benutzeranmeldenamen*). Dies ist ein Anmeldename für Benutzer, der Anmeldenamen im Internet ähnlich ist (optional definiert und eindeutig in der Domäne).

Benutzer und Gruppen

Benutzer und Gruppen sind Windows 2000 Active Directory-Objekte. Jedes Active Directory-Objekt ist eine bestimmte, benannte Attributgruppe, die für etwas Konkretes wie beispielsweise einen Benutzer, einen Drucker oder eine Anwendung steht. Die Attribute enthalten Informationen zu dem Element, für das das Verzeichnisobjekt steht. Attribute für einen Benutzer können beispielsweise den zugeordneten Benutzernamen, den Nachnamen und die E-Mail-Adresse enthalten.

Wie in anderen Betriebssystemen vereinfachen Gruppen die Benutzerverwaltung, indem sie die Steuerung von Berechtigungen

und den Zugriff auf Ressourcen, Objekte und Attribute auf Gruppenebene anstatt auf Benutzerebene ermöglichen. Gruppen sind Active Directory-Objekte oder Objekte auf dem lokalen System, die Benutzer, Kontakte, Computer und andere Gruppen enthalten können. Gruppen können für folgende Aufgaben verwendet werden:

- Verwaltung des Zugriffs von Benutzern und Computern auf gemeinsame Ressourcen wie beispielsweise Active Directory-Objekte und deren Merkmale, SHARE-Ressourcen im Netzwerk, Dateien, Verzeichnisse, Druckwarteschlangen usw.
- Erstellen einer E-Mail-Verteilerliste
- Filtern von Gruppenrichtlinien

Gruppen können zu Sicherheitszwecken (Zugriffssteuerung und -richtlinie) bzw. zu Gruppierungszwecken (Verteilerlisten) verwendet werden. Wenn Sie eine Gruppe erstellen, müssen Sie angeben, ob diese zu Sicherheitszwecken verwendet wird.

Jeder Benutzer gehört mindestens einer Gruppe, der so genannten primären Gruppe an. Aus einer Reihe von Windows 2000-definierten Gruppen, die sich standardmäßig im Kontext *Domäne/Benutzer* befinden, können Sie eine Gruppe auswählen und als primäre Gruppe definieren. All diese Gruppen haben das Präfix "**Domäne**." Sie können Benutzern auch andere definierte Gruppen zuordnen. Weitere Informationen hierzu finden Sie im Abschnitt "Gruppen verwalten" in der MSDN-Dokumentation von Microsoft.

Tivoli unter Windows 2000 verwenden

Wenn Sie Windows 2000 Active Directory einen Benutzer hinzufügen, wird in dem Domänencontainer der Domäne, in der sich der Benutzerdatensatz befindet, ein Benutzerobjekt erstellt.

In der folgenden Tabelle finden Sie die Merkmalwerte, die Sie beim Erstellen eines Benutzers mindestens angeben müssen. Die einzigen Elemente, die Sie angeben müssen sind: der allgemeine Name (**CN**), **Kontext** und der **SAM-Kontoname**. Die anderen Elemente können auf die Standardwerte gesetzt werden (solch ein Konto ist jedoch für die Verwendung mit Active Directory wenig hilfreich).

Merkmal	Wert
Vollständiger Name	Leer
Allgemeiner Name (CN)	Muss explizit angegeben werden
Kontext	Muss explizit angegeben werden
Vorname	Leer
Nachname	Leer
Benutzer-Principal-Name (UPN)	Leer
SAM-Kontoname	Muss explizit angegeben werden
Kennwort	Leer
Benutzer muss Kennwort ändern	WAHR
Benutzer kann Kennwort nicht ändern	FALSCH
Kennwort läuft nie ab	FALSCH
Konto deaktiviert	WAHR
Gruppe	Domänenbenutzer
Profil	Leer
Konto läuft nie ab	WAHR

Windows 2000 Active Directory unterstützt für Objektnamen mehrere Formate. Diese Formate berücksichtigen die unterschiedlichen Namensformate, die von der ursprünglichen Anwendung abhängen. Die Verwaltungs-Tools von Active Directory zeigen Zeichenfolgen für Namen in einem Standardformat an. Hierbei handelt es sich um den so genannten *kanonischen* Namen.

Die Windows 2000-Benutzerschnittstelle zeigt standardmäßig Objektnamen an, die den kanonischen Namen verwenden, der die relativ definierten Namen auflistet (von **root** abwärts und ohne die RFC 1779-Benennungsattributdeskriptoren). Sie verwendet den DNS-Domänennamen (das Namensformat, in dem die Domänenkennungen durch Punkte voneinander getrennt sind).

Beispielsweise könnte ein LDAP-registrierter Name in folgendem kanonischen Format angezeigt werden:

```
noam.reskit.com/marketing/promotions/jsmith
```

In diesem Fall besteht der kanonische Name aus dem allgemeinen Namen (cn) **jsmith**. Diese Person ist in der Organisationseinheit (ou) **marketing** tätig mit den Domänenkomponenten (dc) **noam**, **reskit** und **com** (ganz links steht der Name des Blattobjekts und ganz rechts der Name des Roots.)

Tivoli SecureWay User Administration verwendet das kanonische Namensformat von Active Directory für die Attribute **w2k_context**, **w2k_manager** und **w2k_membersof**.

Anmerkung: Eine Ausnahme ist der Name der primären Gruppe unter dem Attribut 'w2k_membersof', der nicht im kanonischen Format angegeben wird.

Weitere Informationen zum Erstellen eines Windows 2000-Benutzerkontos in Tivoli SecureWay User Administration finden Sie unter „Informationen zu Windows 2000-Benutzerkonten" auf Seite 180.

Novell NetWare-Verzeichnisdienst

Beim NetWare-Verzeichnisdienst (NDS = NetWare Directory Services) handelt es sich um einen Informationsdatenbankdienst, der mit dem Release NetWare 4.0 eingeführt wurde und Netzwerkressourcen wie beispielsweise Benutzer, Gruppen, Drucker, Datenträger und andere physische Netzwerkeinheiten in einer hierarchischen Baumstruktur verwaltet. NDS verfügt über Einrichtungen zum Speichern, Abrufen, Verwalten und Verwenden von Informationen zu Netzwerkressourcen. Die NDS-Informationen werden nicht auf einem einzigen Server gespeichert, sondern über eine globale Datenbank verteilt und können von allen Servern abgerufen werden. Diese Datenbank ist die NetWare Directory-Informationsdatenbank. Die Datenbank verwaltet Ressourcen in einer hierarchischen Baumstruktur. Benutzer und Systemadministratoren können auf alle Netzwerkdienste zugreifen, ohne den physischen Standort des Servers, der den Dienst speichert, kennen zu müssen. Die Bezeichnung *Verzeichnis* im NetWare-Verzeichnisdienst bezieht sich auf die globale Datenbank.

Objekte im NetWare-Verzeichnisdienst

NDS ist objektorientiert. Physische Einheiten werden durch Objekte oder logische Darstellungen physischer Einheiten dargestellt. Benutzer und Gruppen sind logische Benutzer- und Gruppenkonten und bilden eine eigene NDS-Objektart. Das Arbeiten auf einem objektorientierten System hat u.a. den Vorteil, dass das Versetzen einer Einheit nicht die Objektdefinition ändert. Dies erleichtert die Systemverwaltung ungemein.

Benutzeranmeldung und Authentifizierung

Da NDS im Netzwerk verteilt wird und sich nicht auf einem bestimmten Server befindet, melden sich NDS-Benutzer am Netzwerk und nicht an einem Server an. Wenn der Benutzer auf Netzwerkressourcen zugreift, werden im Hintergrund Authentifizierungsprozesse ausgeführt, die überprüfen, ob der Benutzer dazu berechtigt ist, auf diese Ressourcen zuzugreifen. Die Authentifizierung ermöglicht dem Benutzer, auf alle Server, Datenträger, Drucker usw. im Netzwerk zuzugreifen, für die er über Berechtigungen verfügt. Benutzer-Trustee-Berechtigungen im Verzeichnis beschränken den Zugriff der Benutzer im Netzwerk. Anhand der Authentifizierung kann überprüft werden, ob ein Benutzer dazu berechtigt ist, Verzeichnis- und Dateisystemressourcen zu verwenden. Die Authentifizierung und die Zugriffssteuerunglisten (ACL) gewährleisten gemeinsam die Netzwerksicherheit.

Benutzer und Gruppen

Benutzer und Gruppen sind Objekte innerhalb der NDS-Struktur. Beim Erstellen eines Benutzers muss ein Container ausgewählt werden, dem der zu erstellende Benutzer zugeordnet wird. Benutzerobjekte erhalten alle NDS-Berechtigungen und Trustee-Zuordnungen des Containers, dem sie zugeordnet werden. Zur Vereinfachung des Benutzerzugriffs auf Anwendungen und Ressourcen können Gruppen erstellt werden.

Benutzer und Gruppen werden *Trustees* genannt, wenn sie über NetWare-Merkmale oder -Werte verfügen. Zugriffsrechte können Benutzern oder Gruppen zugeordnet werden; nachdem die Zugriffsrechte zugeordnet wurden, werden sie Trustee-*Zuordnungen* genannt.

Diese Zuordnungen werden *direkte Zuordnungen* genannt, wenn sie den Benutzern oder Gruppen direkt zugeordnet wurden.

Wenn ein Benutzer einer Gruppe zugeordnet wird, erhält der Benutzer die Trustee-Zuordnungen, die der Gruppe zugeordnet wurden.

Tivoli unter NetWare verwenden

In Tivoli SecureWay User Administration ist für die Kommunikation mit einem NetWare-NDS-Endpunkt die Ausführung des Befehls **wsetnds** erforderlich. Dieser Befehl ermöglicht der Anwendung die Anmeldung an der NetWare-NDS-Baumstruktur. Sie müssen diesen Befehl für jede von Ihnen verwaltete NDS-Baumstruktur ausführen. Wenn Sie diesen Befehl ausgeführt haben, müssen Sie ihn nicht erneut ausführen, es sei denn, Sie ändern den Anmeldenamen oder das Kennwort des angegebenen Kontos. Der Befehl **wsetnds** kann nicht für Systeme mit NetWare 3.*x* verwendet werden, da NetWare 3.*x* NDS-Baumstrukturen nicht unterstützt. Wenn Sie von einem NetWare-Knoten aus Benutzerinformationen weitergeben, können Sie nur die Benutzerinformationen mit einer Kontoart kleiner oder gleich der dem Befehl **wsetnds** zugeordneten Kontoart verwenden.

OS/390-Resource Access Control Facility

RACF (RACF = Resource Access Control Facility) ist ein Sicherheitsdienst, der Benutzern den Zugriff auf geschützte Ressourcen ermöglicht. RACF ist Teil des OS/390 Security Server, der wiederum Teil des Betriebssystems OS/390 ist.

RACF-Datenbank

Die RACF-Datenbank speichert Informationen zu Benutzern, Gruppen, Datensätzen und anderen Ressourcen. Die Datenbanksätze, die diese Objekte beschreiben, haben die Bezeichnung *Profile*. In der RACF-Datenbank befinden sich unterschiedliche Profilarten. Ein Profil zum Schutz einer einzelnen Ressource, beispielsweise eines Transaktions- oder Chiffrierschlüssels, hat die Bezeichnung *Einzelprofil*. Ein Profil zum Schutz mehrerer Ressourcen wird als *generisches Profil* bezeichnet. Die RACF-Datenbank verwendet auch Benutzer- und Gruppenprofile.

Anmerkung: Die RACF-Profile sollten nicht mit den Tivoli Secureway User Adminstration-Profilen verwechselt werden. Weitere Informationen zu den Tivoli SecureWay User Administration-Profilen finden Sie unter „Benutzer- und Gruppenprofile” auf Seite 23.

RACF-Segmente

Bei den Segmenten für RACF-Profile handelt es sich um optionale Erweiterungen des Basisprofils, die Informationen zu einer bestimmten Anwendung bzw. Verwaltungsfunktion enthalten. Wenn der Benutzer beispielsweise das Programm 'Customer Information Control System' (CICS) ausführen muss, benötigt das Benutzerprofil ein CICS-Segment. Möglicherweise benötigen Benutzerprofile weitere Segmente, um die für den Benutzer erforderlichen Aktionen ausführen zu können.

Benutzerauthentifizierung

Wenn sich Benutzer am Betriebssystem anmelden, müssen sie eine gültige Benutzer-ID und ein Kennwort eingeben. RACF unterstützt auch Alternativen zum herkömmlichen Kennwort. RACF unterstützt beispielsweise *Passtickets*. Ein 'Passticket' kann von RACF oder einer anderen Funktion, die über entsprechende Berechtigungen verfügt, generiert und nur ein einziges Mal innerhalb eines begrenzten Zeitraums auf einem bestimmten System verwendet werden. Bei der Benutzerauthentifizierung überprüft RACF Folgendes:

- Ob der Benutzer für RACF definiert ist.
- Ob der Benutzer ein gültiges Kennwort oder eine gültige Alternative, beispielsweise ein 'Passticket', angegeben hat.
- Ob die Benutzer-ID (UID) und Gruppen-ID (GID) unter OS/390 gültig sind.
- Ob der Benutzer-ID der Status 'Widerrufen' zugeordnet ist. Ist dies der Fall, wird ein RACF-definierter Benutzer daran gehindert, auf das System bzw. auf bestimmte Gruppen zuzugreifen.
- Ob der Benutzer das System an diesem Tag bzw. zu dieser Zeit verwenden darf.
- Ob der Benutzer auf das Terminal zugreifen darf.

Ressourcenberechtigung

Wenn der Benutzer den Zugriff auf eine Ressource anfordert, gibt die Systemressourcenverwaltung eine RACF-Anforderung aus, um zu prüfen, ob der Benutzer dazu berechtigt ist, auf die Ressource zuzugreifen. RACF überprüft das Profil, das die Informationen zu der angeforderten Ressource in der RACF-Datenbank enthält. RACF übergibt diese Informationen an die Systemressourcenverwaltung. Auf Grundlage dieser Informationen erteilt bzw. verweigert die Systemressourcenverwaltung den angeforderten Zugriff.

RACF-Benutzerattribute

Benutzer mit verschiedenen Job-Berechtigungsklassen benötigen unterschiedliche Zugriffsberechtigungen für Ressourcen. Über die RACF-Benutzerattribute können einem Benutzer Sonderzugriffsberechtigungen für Ressourcen erteilt werden. Durch die Benutzerattribute ist auch festgelegt, was ein Benutzer mit der RACF-Datenbank machen darf. Es folgen Beispiele für grundlegende RACF-Benutzerattribute:

- SPECIAL—Dieses Benutzerattribut wird RACF-Administratoren zugeordnet, die dazu berechtigt sind, alle RACF-Befehle zu verwenden und sämtliche Profilarten in der RACF-Datenbank zu definieren. Das Attribut RACF SPECIAL ermöglicht dem Benutzer, den Inhalt der RACF-Datenbank zu verwalten. Dem Benutzer werden jedoch für den Zugriff auf die anderen OS/390-Ressourcen keine Sonderberechtigungen erteilt, die über die Berechtigungen eines normalen Benutzers hinausgehen.
- OPERATIONS—Dieses Benutzerattribut ermöglicht dem Benutzer den Zugriff auf alle Datensätze und einige zusätzliche Ressourcenklassen im System. Außerdem ermöglicht dieses Attribut dem Benutzer das Anlegen von Datensätzen für andere Benutzer im System. Aus Sicherheitsgründen sollte dieses Attribut nur temporären Benutzer-IDs zugeordnet werden, die in Notfällen geöffnet werden.
- AUDITOR—Dieses Benutzerattribut wird Benutzern zugeordnet, die für die Überwachung der RACF-Datenbank sowie der Systemprotokolle und der Systemintegrität zuständig sind. Das Attribut AUDITOR berechtigt den Benutzer, alle Profile in der

RACF-Datenbank einzusehen und die Prüfattribute für das System und für Einzelprofile zu ändern.

- REVOKE—Über dieses Benutzerattribut kann ein RACF-definierter Benutzer daran gehindert werden, das System zu verwenden. Das Attribut REVOKE kann ausgelöst werden, wenn ein Benutzer zu oft das falsche Kennwort eingibt oder sich eine bestimmte Zeit lang (eine vorgegebene Anzahl an Tagen) nicht am System anmeldet. Dieses Attribut kann auch angewendet werden, wenn ein Administrator das Profil eines Benutzers widerruft.

RACF-Gruppen

Jeder RACF-Benutzer gehört mindestens einer RACF-Gruppe an. Ein Benutzer, der einer Gruppe angehört, ist mit der Gruppe *verbunden*. RACF-Gruppen können unterschiedlichen Zwecken dienen. RACF-Gruppen dienen normalerweise folgenden Zwecken:

- Mit Hilfe von **Ressourcenschutzgruppen** können Sie Datensätze schützen. Es gibt zwei Arten von Datensätzen: Benutzerdatensätze und Gruppendatensätze. Das primäre Qualifikationsmerkmal für den Zugriff auf einen Benutzerdatensatz ist die Benutzer-ID. Für alle anderen Datensätze wurde das primäre Qualifikationsmerkmal als RACF-Gruppe definiert. Wenn Sie beispielsweise den Datensatz **CICS41.LOADLIB** schützen möchten, müssen Sie eine Gruppe mit dem Namen **CICS41** definieren. Sie können dann zu Ihrer Sicherheit RACF-Datensatzprofile definieren, die mit **CICS41** beginnen.
- **Administrative Gruppen** können zu Informationszwecken verwendet werden. Üblicherweise werden solche Gruppen zum Erstellen einer Struktur, die die Organisation der Abteilungen und Ressorts Ihres Unternehmens abbildet, verwendet. Sie können dann die Benutzer in einer Abteilung der entsprechenden Gruppe zuordnen. Wenn Sie wissen müssen, welche Personen für eine bestimmte Abteilung arbeiten, können Sie die Gruppe, die für diese Abteilung steht, auflisten.
- **Funktionsgruppen** sind Gruppen für Job-Berechtigungsklassen oder Zuständigkeiten und werden verwendet, um Benutzern ihre Zugriffsberechtigungen zuzuordnen.

Wenn es in Ihrem Unternehmen beispielsweise die Job-Berechtigungsklasse 'Buchhalter' gibt, können Sie die RACF-Gruppe ACCOUNT für diese Berechtigungsklasse erstellen. Sie würden dann alle Buchhalter dieser Gruppe zuordnen in der Annahme, dass diese dieselben Berechtigungen benötigen. Sie würden dann die Gruppe ACCOUNT allen Zugriffslisten für die Ressourcen, auf die die Buchhalter zugreifen müssen, zuordnen.

Die Benutzerattribute SPECIAL, OPERATIONS und AUDITOR können einem Benutzer zugeordnet werden, indem der Benutzer mit einer Gruppe verbunden wird. Wenn diese Attribute über eine Gruppe zugeordnet werden, heißen sie GROUP-SPECIAL, GROUP-OPERATIONS usw. Benutzer mit einem dieser Attribute können mit diesem Attribut nur auf gruppeneigene Ressourcen zugreifen.

Lightweight Directory Access Protocol (LDAP)

LDAP ist ein Verzeichnisdienstprotokoll, das über TCP/IP ausgeführt wird. LDAP vereinfacht den Zugriff auf ein Verzeichnis, da es nicht so komplex ist und weniger Funktionen verwendet. LDAP stellt nicht dieselben Anforderungen an Ressourcen wie X.500 DAP (DAP = Directory Access Protocol).

Tivoli SecureWay User Administration verwaltet die Benutzerdaten in einem Verzeichnis, indem es auf einem verwalteten Knoten einen Proxy ausführt und LDAP zur Kommunikation mit dem Verzeichnis verwendet. Benutzerdaten können alle Informationen zu Benutzern, die im Verzeichnis gespeichert sind, umfassen. Beispiele für solche Informationen sind Kennwörter, Telefonnummern, Titel, Standort des Büros usw. Tivoli SecureWay User Administration kann Benutzerdefinitionen im LDAP-Verzeichnis lesen und diese Daten zum Erstellen und Verwalten von Konten auf allen Systemen, die es verwaltet, verwenden. Tivoli SecureWay User Administration ermöglicht auch die Weitergabe verfügbarer Benutzerdefinitionen an das LDAP-Verzeichnis.

Weitere Informationen hierzu finden Sie in der Dokumentation zu Ihrem Verzeichnisserver.

Funktionsweise der Benutzer- und Gruppenverwaltung

Bei Tivoli SecureWay User Administration handelt es sich um eine auf Profilen basierende Anwendung, die auf verschiedenen Plattformen zum Einsatz kommen kann. Mit der Anwendung Tivoli SecureWay User Administration können UNIX-, Windows NT-, Windows 2000- und NetWare-Benutzerkonten verwaltet werden. Darüber hinaus stehen noch zusätzliche Anwendungspakete für die Verwaltung von OS/390-, OS/400- und OS/2-Konten zur Verfügung. Mit Tivoli SecureWay User Administration können auch UNIX-Gruppen sowie Windows NT- und NetWare-Gruppenzugehörigkeiten verwaltet werden.

Mit Tivoli SecureWay User Administration können Sie Datensätze auf einem beliebigen verwalteten Knoten oder Endpunkt an ein Benutzer- oder Gruppenprofil weitergeben. Wenn Sie die Datensätze des Profils aktualisiert haben, können Sie das Profil an beliebige Subskribenten verteilen. Dazu gehören unter anderem:

- Andere Profilmanager
- Verwaltete Knoten
- NIS-Domänen (NIS = Network Information Services)
- Windows NT-Domänen (verwaltete Knoten oder Endpunkte)
- Windows NT-Workstations (verwaltete Knoten oder Endpunkte)
- NDS-Baumstrukturen (Endpunkte)
- NetWare 3.*x*-Server (Endpunkte)

Tivoli SecureWay User Administration muss mit einem bekannten verwalteten Knoten oder Endpunkt kommunizieren. Wenn Sie auf Ihrem NetWare-Server die Datei **UMBO.NLM** (das NLM (NetWare Loadable Module) von Tivoli SecureWay User Administration) bzw. auf Ihrem Windows NT-Server die ausführbare Datei **UMBO.EXE** installieren, behandelt Tivoli SecureWay User Administration diese Server wie Endpunkte.

Benutzer- und Gruppenprofile

Tivoli SecureWay User Administration verwendet *Benutzer*- und *Gruppenprofile* zur Verwaltung von Benutzern und Gruppen. Sie können ein Profil in einem Profilmanager erstellen und die Standardwertegruppen des Profils definieren. Sie können Tivoli-Ressourcen wie Profilmanager, NIS-Domänen, UNIX-Systeme, Windows NT-Domänen und NetWare-NDS-Baumstrukturen dem Profilmanager zuordnen, der das Profil enthält, und anschließend Kopien des Profils an die Subskribenten verteilen. Wenn die im Profil definierten Benutzer- oder Gruppendatensatzinformationen an ihre Zieladresse, einen Profilendpunkt, verteilt werden, ändert Tivoli SecureWay User Administration die Systemdateien so, dass sie den in den Datensätzen des Profils definierten Informationen entsprechen. Sobald die Systemdateien aktualisiert sind, verwenden andere Dienste wie beispielsweise NIS die aktualisierten Dateien zum Erstellen von neuen Zuordnungen und Datenbanken. Die Verteilung von Benutzer- und Gruppenprofilen kann den Tivoli-Ressourcen über die Grenzen von Tivoli Management Regions (TMRs) hinweg zugeordnet werden, und die Tivoli-Ressourcen können die Verteilungen TMR-übergreifend empfangen.

Ein Benutzerprofil ist eine Gruppe von Benutzerdatensätzen. Jeder Benutzerdatensatz enthält allgemeine Informationen sowie Informationen zu einer oder mehreren Kontoarten (UNIX, Windows NT, Windows 2000 und NetWare) für einen einzelnen Benutzer. Die Benutzerkontodatensätze für Windows NT, Windows 2000 und NetWare umfassen die Gruppenzugehörigkeitsverwaltung.

Ein Gruppenprofil ist eine Gruppe von Gruppendatensätzen. Jeder Gruppendatensatz enthält alle Informationen, die zur Definition von UNIX-Gruppen und deren Mitglieder erforderlich sind. Dazu gehören Informationen wie der Gruppenname, die Gruppen-ID und eine Gruppe von Anmeldenamen für Mitglieder.

Weitere Informationen zur Konfigurationsverwaltung sowie zu Profilen und Profilmanagern finden Sie im *Tivoli Management Framework Benutzerhandbuch*.

Richtlinien für Benutzer- und Gruppenprofile

Tivoli SecureWay User Administration verwendet auf Profilen statt auf Richtlinienbereichen basierende Richtlinien. Das heißt, dass jedes Benutzer- und Gruppenprofil über seine eigenen ***Standardwertegruppen*** und ***Richtlinien für Gültigkeitsprüfung*** verfügt.

Standardwertegruppen legen Standardwerte für Attribute fest, die beim Erstellen neuer Profildatensätze nicht angegeben werden. Richtlinien für Gültigkeitsprüfung legen zulässige Werte für Profildatensätze fest. Weitere Informationen zu Standardwertegruppen und Richtlinien für die Gültigkeitsprüfung finden Sie im *Tivoli Management Framework Benutzerhandbuch*.

Auf Profilen basierende Richtlinien bieten Ihnen mehr Flexibilität bei der Verwaltung Ihrer Benutzerkonten. Wenn beispielsweise in Ihrer Buchhaltungsabteilung andere Anforderungen an Benutzerkonten gestellt werden als in Ihrer Vertriebsabteilung, können Sie zwei unterschiedliche Profile in demselben Profilmanager erstellen, die jeweils unterschiedliche Standardwertegruppen und Richtlinien für Gültigkeitsprüfung haben. Genaue Beispiele dazu, wie diese Flexibilität Ihnen bei der effektiven Verwaltung Ihrer Benutzerkonten helfen kann, finden Sie unter „Große Anzahl Benutzer verwalten” auf Seite 38.

Subskribenten einrichten

Tivoli SecureWay User Administration ermöglicht Ihnen die Angabe der verwalteten Knoten bzw. Endpunkte, die Ziele eines Verteilvorgangs sind. Tivoli SecureWay User Administration erkennt zwei Ebenen von Subskribenten: Subskribenten auf *Profilmanagerebene* und Subskribenten auf *Datensatzebene*.

Die Subskribenten auf Profilmanagerebene legen fest, an welche Endpunkte und Profilmanager Tivoli SecureWay User Administration versucht, den Inhalt des Profils zu verteilen. Die Anwendung verwendet dann die Subskribenten auf Datensatzebene, um zu überprüfen, auf welcher Untergruppe von Endpunkten die Datensätze verarbeitet werden.

Daten an Profile weitergeben

Wenn Sie ein Profil erstellen, ist das Profil nur eine Definition der Informationen, die jeder Profilbestandteil enthält. Die Daten, die die jeweilige Benutzerkontokonfiguration definieren, müssen dann an die Profilbestandteile *weitergegeben* werden (d. h., die Profilbestandteile müssen 'gefüllt' werden). Sie können die Daten von Benutzern von einem oder mehreren Endpunkt(en) an ein Benutzerprofil weitergeben. Sie geben an, von welchen Endpunkten die Informationen abgerufen werden sollen und ob diese Informationen die vorhandenen Profilinformationen überschreiben oder die Benutzerinformationen an das Profil angehängt werden sollen.

Während eines Weitergabevorgangs mit der Option zum Zusammenfügen versucht Tivoli SecureWay User Administration, Benutzerinformationen aus der Quelle in die bereits im Profil vorhandenen Benutzerdatensätze einzufügen. Die Anwendung verwendet den Anmeldenamen als Schlüssel, um festzulegen, ob eine Übereinstimmung vorliegt. Wenn eine Übereinstimmung gefunden wird, vergleicht die Anwendung die Betriebssystemkontoarten. Wenn diese unterschiedlich sind, fügt die Anwendung die Informationen in dem Datensatz zusammen. Sind sie identisch, gibt Tivoli SecureWay User Administration einen Fehler zurück.

Wenn die Benutzerinformationen mit einem Benutzerdatensatz zusammengefügt werden, werden die neuen Benutzerinformationen in den Benutzerdatensatz aufgenommen und die allgemeinen Benutzerinformationen auf Attributbasis zusammengefügt, wobei die im Benutzerdatensatz vorhandenen Informationen Vorrang haben.

Es gibt zum Beispiel einen Datensatz im Profil, in dem **freddie** als Anmeldename des Benutzers definiert ist. Der Datensatz enthält allgemeine Informationen und UNIX-Benutzerinformationen. Es gibt einen Benutzer mit demselben Anmeldenamen in der Windows NT-Domäne, von der aus Sie Daten an das Benutzerprofil weitergeben. Tivoli SecureWay User Administration erkennt, dass diesen beiden Benutzerdatensätzen derselbe Anmeldename zugeordnet ist. Es erkennt außerdem, dass der Anmeldename **freddie** einem UNIX-Konto im Profil und einem Windows NT-Konto auf dem Windows NT-verwalteten Knoten zugeordnet ist. Während des Weitergabevor-

gangs werden die Windows NT-Benutzerinformationen dem vorhandenen Benutzerdatensatz hinzugefügt, und die allgemeinen Benutzerinformationen werden mit denen im Benutzerdatensatz zusammengefügt.

Wenn Sie den Weitergabevorgang über eine NetWare-NDS-Baumstruktur, eine NetWare-Bindeeinheit, eine Windows NT- Domäne oder Windows 2000 Active Directory durchführen, verwendet der erstellte Datensatz den Benutzeranmeldenamen für das NetWare-, Windows NT- oder Windows 2000-Konto als Kennwort. Wenn Sie vor der Verteilung des Profils an die Endpunkte kein Kennwort hinzufügen, wird das Kennwort für das Konto zum Anmeldenamen.

Profile verteilen

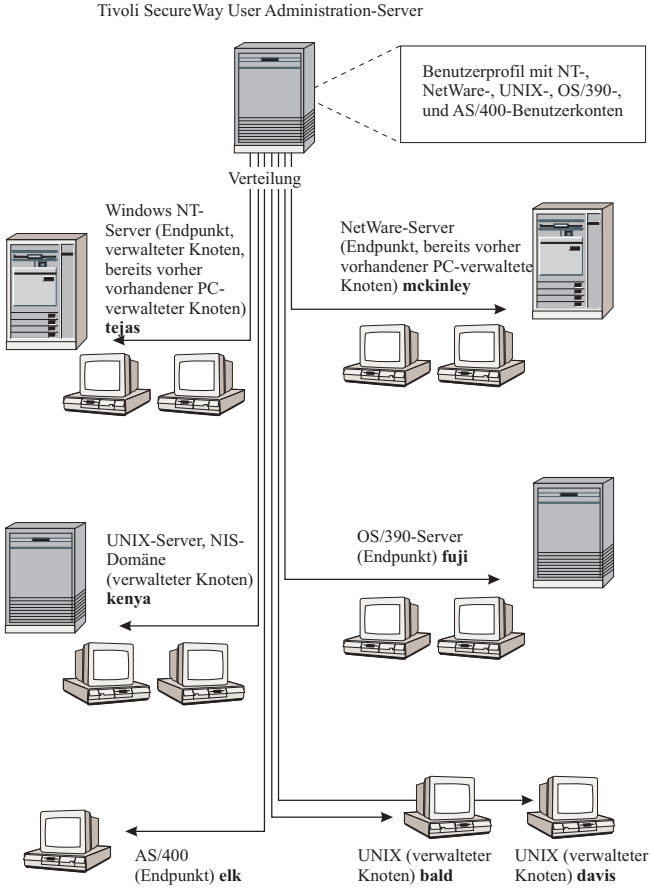
Nachdem Sie Daten an ein Profil weitergegeben, einem Profil neue Datensätze hinzugefügt oder vorhandene Datensätze in einem Profil editiert haben, müssen Sie das Profil an die Endpunkte verteilen, damit die Änderungen wirksam werden. Sie können die Verteilung vom Profilmanager aus durchführen, der die Datensätze aller im Manager gespeicherten Profile verteilt, oder ein einzelnes Profil verteilen.

Ihr Benutzerprofil enthält zum Beispiel drei Benutzerkontodatensätze. Im ersten Benutzerkontodatensatz werden die verwalteten Knoten **olympus**, **mckinley** und **kenya** als Subskribenten aufgelistet. Im zweiten Benutzerkontodatensatz werden die verwalteten Knoten **bald** und **tejas** als Subskribenten aufgelistet. Im dritten Benutzerkontodatensatz wird der verwaltete Knoten **davis** als einziger Subskribent aufgelistet.

Wenn Sie dieses Profil an die verwalteten Knoten **olympus**, **mckinley**, **kenya**, **tejas**, **fuji**, **bald** und **davis** verteilen, werden folgende Verteilungen ausgeführt:

- Alle Datensätze werden an alle Subskribenten verteilt.
- Der erste Benutzerkontodatensatz wird den verwalteten Knoten **olympus**, **mckinley** und **kenya** hinzugefügt.
- Der zweite Benutzerkontodatensatz wird den verwalteten Knoten **bald** und **tejas** hinzugefügt.

- Der dritte Benutzerkontodatensatz wird dem verwalteten Knoten **davis** hinzugefügt.
- Dem verwalteten Knoten **fuji** werden keine Benutzerkontodatensätze hinzugefügt.


Tivoli SecureWay User Administration-Server
Benutzerprofil mit NT-, NetWare-, UNIX-, OS/390-, und AS/400-Benutzerkonten
Verteilung
Windows NT-Server (Endpunkt, verwalteter Knoten, bereits vorher vorhandener PC-verwalteter Knoten) tejas
NetWare-Server (Endpunkt, bereits vorher vorhandener PC-verwalteter Knoten) mckinley
UNIX-Server, NIS-Domäne (verwalteter Knoten) kenya
OS/390-Server (Endpunkt) fuji
AS/400 (Endpunkt) elk
UNIX (verwalteter Knoten) bald
UNIX (verwalteter Knoten) davis

Kennwortsteuerung

Tivoli SecureWay User Administration bietet mehrere Optionen für die Verwaltung von Kennwörtern. Endbenutzer können den Befehl **wpassword -L** verwenden, um ihr Kennwort für alle Subskribentensysteme zu ändern. Administratoren können über die Tivoli-GUI oder mit den Befehlen **wsetusers** und **wpassword -L** Kennwörter verwalten.

Darüber hinaus ermöglicht Tivoli SecureWay User Administration Benutzern die Verwaltung ihrer Kennwörter mit Hilfe des Kennwort-Tools des Betriebssystems, unter dem Ihre Maschine läuft, vorausgesetzt die Richtlinien Ihrer Organisation lassen dies zu. Systemkennwörter werden von Tivoli SecureWay User Administration erst dann aktualisiert, wenn sie explizit im Benutzerprofil geändert wurden oder wenn das Profil im Überschreibmodus verteilt wird. Weitere Informationen zur Steuerung von Kennwörtern finden Sie unter „Kennwortverwaltung” auf Seite 83.

Benutzersuchfunktion

Mit dem Tool ’Benutzersuchfunktion’, das sich auf der Tivoli-Arbeitsoberfläche befindet, können Sie jeden beliebigen Benutzer lokalisieren, den Sie mit Tivoli SecureWay User Administration verwalten.

Für jeden Benutzer im Dialog **Benutzersuchfunktion** gibt es eine erweiterbare Anzeige. Die erweiterte Anzeige eines Benutzers listet alle Profile auf, zu denen der Benutzer gehört. Die aufgeführten Profile folgen der Konvention *Richtlinienbereich Profilmanager Profil*.

Sie können die Benutzerliste durchblättern oder nach einem Benutzer suchen. Sie können die Suche auf einen beliebigen Richtlinienbereich begrenzen oder in Tivoli insgesamt suchen. Die Benutzerliste im Dialog **Benutzersuchfunktion** wird so aktualisiert, dass sie Ihre Suchauswahl enthält.

Nachdem Sie den Benutzer lokalisiert und ein Profil ausgewählt haben (wenn es mehr als ein Profil für diesen Benutzer gibt), können Sie den Benutzerdatensatz editieren. Mit Hilfe der Benutzersuchfunk-

tion können Benutzerdatensätze gefunden und editiert und so schnell aktualisiert werden. Alternativ dazu können Sie das Benutzerprofil öffnen. Dies kann jedoch sehr viel Zeit in Anspruch nehmen, da Benutzerprofile Tausende von Benutzerdatensätze enthalten können. Mit Hilfe der Benutzersuchfunktion können Sie Benutzerdatensätze nicht nur editieren, sondern auch hinzufügen und löschen. Eine vollständige Beschreibung finden Sie im Abschnitt „Benutzerdatensätze suchen” auf Seite 223.

Dateisperren und Kollisionsvermeidung

Gruppenprofile sind während Aktualisierungs-, Weitergabe- und Verteilungsvorgängen gesperrt. Wenn das Profil von einem anderen Administrator zu Aktualisierungszwecken geöffnet wurde, können Sie die Profildatensätze anzeigen. Wenn Sie jedoch versuchen, das gesperrte Profil zu aktualisieren, wird eine Fehlermeldung zurückgegeben, in der der Name des Administrators, der das Profil gesperrt hat, angezeigt wird.

Benutzerprofildatensätze werden während eines Weitergabevorgangs bzw. einer Verteilung gesperrt. Wenn jedoch ein Administrator das Benutzerprofil zum Editieren öffnet, werden die Benutzerprofildatensätze nicht gesperrt. Wenn Sie einen Benutzerdatensatz editieren und ein Administrator zur gleichen Zeit denselben Datensatz aktualisiert, wird die folgende Fehlermeldung ausgegeben, wenn Sie versuchen, Ihre Änderungen zu speichern:

```
Der von Ihnen editierte Datensatz ist älter als der in der Datenbank
gespeicherte Datensatz. Vor dem Speichern muss der Datensatz erneut
editiert werden. Der Dialog zum Editieren wurde aktualisiert und zeigt
jetzt den neueren Datensatz aus der Datenbank an.
```

Sicherheitsverwaltung

Tivoli SecureWay User Administration kann zusammen mit Tivoli SecureWay Security Manager eingesetzt werden, wenn diese Anwendung installiert ist. Tivoli SecureWay Security Manager ermöglicht Ihnen die Implementierung einer umfassenden, konsistenten Sicherheitsrichtlinie für Ihr gesamtes Unternehmen mit einem auf Berechtigungsklassen basierenden Sicherheitsmodell. Diese Berechtigungsklassen entsprechen Jobfunktionen. Mit Tivoli SecureWay

Security Manager definieren Sie, welche Benutzer eine bestimmte Berechtigungsklasse haben, und ordnen auf der Grundlage dieser Berechtigungsklasse Systemressourcen zu oder begrenzen diese. Ausführliche Informationen zum Verwalten von Sicherheitsgruppen und Berechtigungsklassen finden Sie im *Tivoli SecureWay Security Manager Benutzerhandbuch.*

Die Zusammenarbeit zwischen Tivoli SecureWay User Administration und Tivoli SecureWay Security Manager ermöglicht Folgendes:

- Wenn Sie einen Benutzerdatensatz einem Benutzerprofil von Tivoli SecureWay User Administration hinzufügen, haben Sie die Option, diesen Benutzer einer oder mehreren Sicherheitsgruppen in einem oder mehreren Sicherheitsprofilen hinzuzufügen.
- Wenn Sie einen Benutzer einer Sicherheitsgruppe hinzufügen und dieser Benutzer in einem Benutzerprofil verwaltet wird, wird der Benutzerdatensatz so aktualisiert, dass er die neue Sicherheitsgruppe enthält.
- Wenn Sie einen Benutzerdatensatz aus einem Benutzerprofil löschen, wird der Benutzer aus jeder Sicherheitsgruppe entfernt, zu der er gehört.
- Wenn Sie einen Benutzer aus einer Sicherheitsgruppe löschen, wird die Sicherheitsgruppe aus dem Benutzerdatensatz im zugeordneten Benutzerprofil entfernt. Wenn derselbe Benutzer Benutzerdatensätze in mehreren Benutzerprofilen hat, wird nur der Benutzerdatensatz im zugeordneten Benutzerprofil aktualisiert, alle anderen werden nicht geändert.
- Wenn Sie einen Benutzerdatensatz von einem Benutzerprofil in ein anderes verschieben, werden alle Sicherheitsgruppen, zu denen der Benutzer gehört, mit dem Namen des neuen Benutzerprofils aktualisiert.

Jeder Benutzerdatensatz kann mehreren Sicherheitsgruppen in mehreren Sicherheitsprofilen zugeordnet werden; innerhalb einer Sicherheitsgruppe ist ein Benutzereintrag jedoch nur jeweils einem einzigen Benutzerdatensatz zugeordnet. Wenn ein Benutzer in Ihrem Unternehmen in mehrere Benutzerdatensätze aufgenommen wurde, werden daher Änderungen an einer Sicherheitsgruppe nur in dem

zugeordneten Benutzerdatensatz widergespiegelt. Tivoli SecureWay Security Manager hat keine Möglichkeit, andere Benutzerdatensätze für denselben Benutzer zu erkennen.

Task-spezifische Berechtigungsklassen

Tivoli SecureWay User Administration stellt eine Reihe von *Task-spezifischen Berechtigungsklassen* zur Verfügung, mit deren Hilfe leitende Administratoren fest definierte Verwaltungsaufgaben an untergeordnete Administratoren delegieren können. Die Task-spezifischen Berechtigungsklassen teilen den Funktionsumfang der Berechtigungsklassen **admin** und **user** auf; sie können statt der von Tivoli Management Framework zur Verfügung gestellten Berechtigungsklassen verwendet werden.

Im Folgenden einige Beispiele für den Einsatz der Task-spezifischen Berechtigungsklassen:

- Help Desk-Mitarbeitern kann die Berechtigung zum Ändern von Kennwörtern, des Standorts des Büros oder der Telefonnummer von Endbenutzern erteilt werden; darüber hinaus erhalten sie keine Möglichkeit zum Ändern von Benutzerkonten.
- Einem für UNIX-Konten zuständigen Administrator kann die Berechtigung zum Ändern UNIX-spezifischer Attribute erteilt werden, während er Windows NT-, Windows 2000- und NetWare-Attribute lediglich anzeigen kann.
- Einem Administrator kann die Berechtigung zum Erstellen neuer Konten, nicht aber zum Löschen vorhandener Konten erteilt werden.

In der folgenden Tabelle werden die Task-spezifischen Berechtigungsklassen gemäß den Operationsarten, die von ihnen zugelassen werden, in Kategorien eingeteilt:

Aktivität	Task-spezifische Berechtigungsklassen
Daten an Benutzerprofile weitergeben (Benutzerprofile mit Daten füllen)	**Admin_Pop_Profile**

Aktivität	Task-spezifische Berechtigungsklassen
Benutzerkennwort ändern	**Admin_Mod_Password**
Mit Kontodatensätzen arbeiten	**Admin_Add_Account** **Admin_Del_Account** **Admin_Edit_Account** **Admin_Mod_Account** **Admin_Mod_Account_Person** **Admin_View_Account**
Kontospezifische Änderungen an Datensätzen vornehmen	**Admin_Mod_Account_LDAP** **Admin_Mod_Account_NT** **Admin_Mod_Account_NW** **Admin_Mod_Account_OS2** **Admin_Mod_Account_OS4** **Admin_Mod_Account_RF** **Admin_Mod_Account_UX** **Admin_Mod_Account_W2K**

Die Task-spezifischen Berechtigungsklassen arbeiten auf derselben Ebene wie die Berechtigungsklasse **admin** (ausgenommen die Berechtigungsklasse **Admin_View_Account**, die auf derselben Ebene wie die Berechtigungsklasse **user** arbeitet). Ist einem Administrator die Berechtigungsklasse **admin** zugeordnet, sollten Sie diesem daher keine Task-spezifische Berechtigungsklasse zuweisen, da mit der Berechtigungsklasse **admin** alle Vorgänge ausgeführt werden können, die durch die Task-spezifischen Berechtigungsklassen eigentlich ausgeschlossen werden sollen.

Mit der Berechtigungsklasse **admin** können Administratoren unter anderem Benutzerdatensätze erstellen, löschen und editieren, Benutzerprofile verteilen und den Inhalt eines Benutzerprofils mit Systemdateien abgleichen. Angenommen, Sie ordnen einem Administrator die Berechtigungsklassen **Admin_Add_Account** und **Admin_Mod_Account** zu, um ihm das Löschen von Datensätzen zu verwehren, weisen ihm aber zusätzlich noch die Berechtigungsklasse **admin** zu, damit er Benutzerprofile verteilen kann. Der Administrator erhält durch die Berechtigungsklasse **admin** weiterhin die Möglichkeit, Benutzerdatensätze zu löschen.

Anmerkung: Tivoli-Administratoren, die die grafische Benutzerschnittstelle (GUI) von Tivoli SecureWay User Administration benötigen, muss *zusätzlich zu* den zugewiesenen Task-spezifischen Berechtigungsklassen mindestens noch die Tivoli-Berechtigungsklasse **user** zugeordnet werden.

Berechtigungsklassen für Benutzerprofile

Die Berechtigungsklasse **Admin_Pop_Profile** ermöglicht Administratoren die Weitergabe von Daten an Benutzerprofile (d. h. das Füllen von Benutzerprofilen mit Daten) über die Tivoli-Arbeitsoberfläche und über den Befehl **wpopusrs**. Detaillierte Informationen zum Füllen von Benutzerprofilen finden Sie unter „Daten an Benutzerprofile weitergeben" auf Seite 144.

Berechtigungsklassen für Kennwortänderungen

Für den Aufruf der administratorspezifischen Version des Befehls **wpasswd** benötigten Tivoli-Administratoren bisher die TMR-Berechtigungsklasse **admin**. Mit dieser Berechtigungsklasse erhielt der Administrator die Möglichkeit, alle Benutzerprofile, die den angegebenen Anmeldenamen enthielten, sowie alle Subskribenten dieser Benutzerprofildatensätze zu aktualisieren. Die administratorspezifische Version des Befehls **wpasswd** konnte daher auch für die Synchronisation von Kennwörtern verwendet werden, während gleichzeitig verhindert wurde, dass Kunden Administratorzugriffe im Zusammenhang mit Kennwortänderungen beeinflussen oder einschränken konnten.

Die Berechtigungsklasse **Admin_Mod_Password** ermöglicht die Ausführung der administratorspezifischen Version des Befehls **wpasswd**, gestattet darüber hinaus jedoch keine Aktionen, für die in der Regel die Berechtigungsklasse **admin** erforderlich ist. Inwieweit der vom Administrator abgesetzte Befehl **wpasswd** ausgeführt wird, hängt davon ab, auf welche Benutzerprofile mit dem angegebenen Anmeldenamen der Administrator Zugriff hat. Beispiel:

- Verfügt der Administrator über die Berechtigungsklasse **admin** oder **Admin_Mod_Password**, werden die Änderungen an den Benutzerprofilen erfolgreich vorgenommen.

- Bei Anforderung einer sofortigen Weitergabe durch Angabe der Argumente **-l** oder **-L** bei Befehl **wpasswd** gilt dasselbe auch für die Subskribenten der Benutzerprofildatensätze.

  Mit der Berechtigungsklasse **Admin_Mod_Password** kann der Administrator keine Kennwörter über den Befehl **wsetusr** oder den Dialog **Benutzerprofilmerkmale** der Tivoli-Arbeitsoberfläche ändern. Um dem Administrator dies zu ermöglichen, muss ihm die Berechtigungsklasse **Admin_Edit_Account**, **Admin_Mod_Account** oder eine bzw. mehrere Berechtigungsklassen zugeordnet werden, die Änderungen an Endpunktattributen erlauben. Weitere Informationen zur Steuerung von Kennwörtern finden Sie unter „Kennwortverwaltung” auf Seite 83.

Berechtigungsklassen für globale Attributänderungen

Die Task-spezifischen Berechtigungsklassen dieser Kategorie ermöglichen Administratoren das Hinzufügen, Löschen und Anzeigen von Benutzerdatensätzen. Darüber hinaus erlauben sie auch die Änderung von Attributen in einem Benutzerdatensatz. Diese Berechtigungsklassen gelten für die Tivoli-Arbeitsoberfläche und die Befehle **wcrtusr**, **wdelusr**, **wgetusr**, **wlsusrs**, **wsetusr** und **wsetusrs**.

Im Unterschied zu herkömmlichen Berechtigungsklassen sind die Task-spezifische Berechtigungsklassen, die Administratoren globale Änderungen an Konten ermöglichen, hierarchisch gegliedert. Die Berechtigungsklasse **Admin_Edit_Account** stellt die höchste Ebene dar, sie ermöglicht das Hinzufügen, Ändern und Anzeigen von Benutzerdatensätzen. Die Berechtigungsklassen **Admin_Add_Account**, **Admin_Delete_Account** und **Admin_Mod_Account** gehören der nächsten Ebene an. Alle drei Berechtigungsklassen zusammen entsprechen der Berechtigungsklasse **Admin_Edit_Account**. Die Berechtigungsklasse **Admin_View_Account** stellt die unterste Ebene dar, sie ermöglicht Administratoren lediglich die Anzeige von Datensätzen.

Die folgende Liste gibt eine Übersicht über den Wirkungsbereich der einzelnen Task-spezifischen Berechtigungsklassen dieser Kategorie:

Admin_Edit_Account Berechtigt den Administrator zum Editieren, Hinzufügen, Ändern, Löschen und Anzeigen von Benutzerdatensätzen.

Admin_Add_Account Berechtigt den Administrator lediglich zum Hinzufügen und Anzeigen von Benutzerdatensätzen.

Admin_Mod_Account Berechtigt den Administrator lediglich zum Ändern der Attribute vorhandener Benutzerdatensätze und zum Anzeigen von Datensätzen.

Anmerkung:
Die Berechtigungsklasse **Admin_Mod_Account** ermöglicht Administratoren die Änderung aller Attribute in einem Benutzerdatensatz, einschließlich globaler sowie endpunktspezifischer Attribute. Verfügt ein Administrator über diese Berechtigungsklasse, müssen ihm keine weiteren Berechtigungsklassen für die Änderung von Endpunktattributen zugeordnet werden.

Admin_Mod_Account_Person Gibt an, dass der Administrator nur diejenigen Attribute vorhandener Benutzerdatensätze ändern kann, die allgemeine Informationen enthalten, wie beispielsweise den Standort des Büros des Benutzers, die Telefonnummer oder Pagernummer.

Admin_Delete_Account Berechtigt den Administrator lediglich zum Löschen und Anzeigen von Benutzerdatensätzen.

Admin_View_Account Berechtigt den Administrator lediglich zum Anzeigen von Benutzerdatensätzen.

Berechtigungsklassen für Änderungen an Endpunktattributen

Die Task-spezifischen Berechtigungsklassen dieser Kategorie ermöglichen es Administratoren, die Attribute der angegebenen Endpunktart zu editieren. Sie berechtigen nicht zu Änderungen an globalen oder allgemeinen Attributen, und es können mit diesen Berechtigungsklassen auch keine neuen Datensätze erstellt werden, die lediglich endpunktspezifische Attribute enthalten. Diese Berechtigungsklassen erlauben lediglich den Zugriff auf die Befehle **wsetusr** und **wsetusrs**.

Die folgende Liste enthält eine Übersicht über die einzelnen Berechtigungsklassen dieser Kategorie sowie die jeweilige Endpunktart, für die sie gelten:

Admin_Mod_Account_LDAP
Berechtigt Administratoren ausschließlich zum Editieren von LDAP-Attributen (LDAP = Lightweight Directory Access Protocol). Diese Task-spezifische Berechtigungsklasse steht nur bei der Installation von Tivoli SecureWay User Administration for LDAP zur Verfügung.

Admin_Mod_Account_NT Berechtigt Administratoren ausschließlich zum Editieren von Windows NT-Attributen. Diese Task-spezifische Berechtigungsklasse wird zusammen mit Tivoli SecureWay User Administration installiert.

Admin_Mod_Account_NW Berechtigt Administratoren ausschließlich zum Editieren von NetWare-Attributen. Diese Task-spezifi-

	sche Berechtigungsklasse wird zusammen mit Tivoli SecureWay User Administration installiert.
Admin_Mod_Account_OS2	Berechtigt Administratoren ausschließlich zum Editieren von OS/2-Attributen. Diese Task-spezifische Berechtigungsklasse steht nur bei der Installation von Tivoli SecureWay User Administration for OS/2 zur Verfügung.
Admin_Mod_Account_OS4	Ermöglicht Administratoren das Editieren von AS/400-Attributen. Diese Task-spezifische Berechtigungsklasse steht nur bei der Installation von Tivoli SecureWay User Administration for AS/400 zur Verfügung.
Admin_Mod_Account_RF	Ermöglicht Administratoren das Editieren von OS/390-Attributen. Diese Task-spezifische Berechtigungsklasse steht nur bei der Installation von Tivoli SecureWay User Administration for OS/390 zur Verfügung.
Admin_Mod_Account_UX	Berechtigt Administratoren ausschließlich zum Editieren von UNIX-Attributen. Diese Task-spezifische Berechtigungsklasse wird zusammen mit Tivoli SecureWay User Administration installiert.
Admin_Mod_Account_W2K	Berechtigt Administratoren ausschließlich zum Editieren von Windows 2000-Attributen. Diese Task-spezifische Berechtigungsklasse wird zusammen mit Tivoli SecureWay User Administration installiert.

Beim Erweitern von Tivoli SecureWay User Administration um Tivoli AEF (Application Extension Facility) und Hinzufügen neuer Kontoarten mit dem Befehl **waddusreptype** stehen zusätzliche Task-spezifische Berechtigungsklassen zur Verfügung. Weitere Informationen finden Sie unter „Tivoli SecureWay User Administration anpassen" auf Seite 345 und in der Beschreibung des Befehls **waddusreptype** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Große Anzahl Benutzer verwalten

Wenn Sie eine große Anzahl von Benutzern mit Tivoli SecureWay User Administration verwalten, ist es sehr wichtig, dass Sie eine sinnvolle Strategie für die Verwendung von Profilmanagern und Profilen einsetzen. Sie sollten Profilmanager und Profile so verwenden, wie eine Sekretärin die einzelnen Fächer und Ordner ihrer Ablage verwendet. Jedes Fach enthält bestimmte Akten, und die Akten sind gut beschriftet und enthalten eine übersichtliche Menge an Informationen. Es wäre nicht sehr effizient, einen Profilmanager und ein Profil für die Verwaltung jedes Benutzers zu erstellen.

Tausende Benutzer derselben Abteilung verwalten

Die Hightide Insurance Corporation (eine fiktive Firma) hat 10.000 Sachbearbeiter angestellt. Diese Sachbearbeiter haben alle Windows NT- und NetWare-Konten. Jeder Sachbearbeiter wird einer bestimmten Region der Vereinigten Staaten zugeordnet: Nordosten (Northeast), Südosten (Southeast), mittlerer Westen (Midwest), Südwesten (Southwest) oder Nordwesten (Northwest). Die Firma hat eine NDS-Baumstruktur mit Kontexten für jede Region und Windows NT-Domänen für jede Region.

Auf der Grundlage der aktuellen Struktur der Hightide Insurance Corporation wäre ein guter Ansatz für die Benutzer- und Gruppenverwaltung von Tivoli SecureWay User Administration die Erstellung eines Profilmanagers für jede geographische Region. Erstellen Sie in jedem Profilmanager die erforderlichen Profile. Mit den folgenden Schritten werden die Profilmanager sowie die Profile erstellt, die Attribute für die Profile festgelegt, Daten an die Profile weitergegeben und die Benutzer an die Endpunkte verteilt.

1. Erstellen Sie die Profilmanager **Northeast**, **Southeast**, **Midwest**, **Southwest** und **Northwest** im Richtlinienbereich **Hightide-region**.
2. Erstellen Sie ein einzelnes Benutzerprofil in einem der Profilmanager.
3. Definieren Sie die Standardwertegruppen für dieses Profil. Da alle Benutzerdatensätze gleich sein müssen, wird diese Standardwertegruppe jedem Profil zugeordnet.
4. Klonen Sie dieses Profil, bis jeder Profilmanager die erforderliche Anzahl Profile enthält.
5. Legen Sie die Richtlinien für Gültigkeitsprüfung für jedes Profil fest. Die Richtlinien für Gültigkeitsprüfung sollten so festgelegt werden, dass nur Benutzer, deren Nachnamen mit den jeweiligen Buchstaben beginnen, in dem Profil vorhanden sein dürfen. Dies müssen Sie für jedes Profil einzeln festlegen.
6. Geben Sie die Benutzerdaten aus den entsprechenden NDS-Kontexten und Windows NT-Domänen an jedes Benutzerprofil weiter. Durch die für jedes Profil festgelegten Richtlinien für Gültigkeitsprüfung können an das Profil nur die Benutzer weitergegeben werden, deren Nachnamen in dem zulässigen Namensbereich liegen.
7. Prüfen Sie, ob die jedem Profil hinzugefügten Benutzerdatensätze korrekt sind. Nehmen Sie gegebenenfalls erforderliche Änderungen an den Benutzerdatensätzen vor.
8. Legen Sie die Standardwerte für die Verteilung für jedes Profil fest. Über diese Standardwerte wird die Verteilungsart festgelegt.
9. Planen Sie die Verteilungen so, dass sie nicht während der Geschäftszeiten ausgeführt werden.

Tausende Benutzer unterschiedlicher Abteilungen verwalten

Die NoonTide Corporation (eine fiktive Firma) hat 10.000 Angestellte. Die Firma ist in verschiedene Abteilungen unterteilt, wie Marketing (Marketing), Vertrieb (Sales), Entwicklung (Development), Qualitätskontrolle (Verification), Unterstützung (Support), Design (Design) und Buchhaltung (Accounting). Die Firma hat eine NDS-Baumstruktur mit Kontexten für jeden Unternehmensbereich, Windows NT-Domänen für jeden Unternehmensbereich und UNIX-NIS-Domänen für die Entwicklungs- und die Qualitätskontrollabteilung.

Die Mitglieder der Entwicklungs- und der Qualitätskontrollabteilung sind jeweils einem bestimmten Projekt zugeordnet, die Mitglieder der Marketingabteilung sind entweder dem Unternehmensmarketing oder einer Region zugeordnet, und jedes Mitglied des Vertriebs ist einer anderen Region zugeordnet.

Die Struktur der NoonTide Corporation bietet eine gute Strategie für die Erstellung von Profilmanagern und Profilen. Führen Sie folgende Schritte aus, um Profilmanager für jede Abteilung zu erstellen und dann Profile für jeden Bereich innerhalb einer Abteilung zu erstellen.

1. Erstellen Sie die Profilmanager **Accounting**, **Design**, **Development**, **Marketing**, **Sales**, **Support** und **Testing** im Richtlinienbereich **Noon-region**.
2. Erstellen Sie ein einzelnes Benutzerprofil in jedem Profilmanager. Dieses Profil wird jeweils zum Hauptprofil der Profilmanager.
3. Definieren Sie die Standardwertegruppen und Richtlinien für Gültigkeitsprüfung für das Hauptprofil jedes Profilmanagers. Da diese Profilmanager unterschiedliche Unternehmensbereiche darstellen, ist es wahrscheinlich, dass sie unterschiedliche Standardwertegruppen und Richtlinien für Gültigkeitsprüfung haben.

4. Klonen Sie das Hauptprofil in jedem Profilmanager, bis Sie alle erforderlichen Profile erstellt haben.
5. Erstellen Sie eine Liste der Benutzer, die in jedes Profil gehören. Sie können beispielsweise die Firmendatenbank der Mitarbeiter oder eine Firmentelefonliste verwenden, um diese Liste zu erstellen. Sie müssen für jedes Profil eine andere Liste erstellen. Der Befehl **wpopusrs** verwendet diese Listen, um an jedes Profil die entsprechenden Benutzerdatensätze weiterzugeben.
6. Verwenden Sie den Befehl **wpopusrs**, um Daten an alle Profile weiterzugeben. Mit der Option **–f** des Befehls **wpopusrs** können Sie eine Datei angeben, die als Definition der Benutzer für dieses Profil verwendet werden soll.
7. Prüfen Sie, ob die jedem Profil hinzugefügten Benutzerdatensätze korrekt sind. Nehmen Sie gegebenenfalls erforderliche Änderungen an den Benutzerdatensätzen vor.
8. Legen Sie die Standardwerte für die Verteilung für jedes Benutzerprofil fest. Über diese Standardwerte wird die Verteilungsart festgelegt.
9. Planen Sie die Verteilungen so, dass sie nicht während der Geschäftszeiten ausgeführt werden.

2

Tivoli SecureWay User Administration installieren

In diesem Kapitel wird erklärt, wie die Tivoli SecureWay User Administration-Software installiert, aktualisiert und deinstalliert wird. Es enthält folgende Abschnitte:

- Tivoli SecureWay User Administration - Installationspakete
- Softwareoptionen und -voraussetzungen sowie Hardwarevoraussetzungen
- Mit Tivoli Software Installation Service (SIS) installieren
- Tivoli SecureWay User Administration installieren
- Tivoli SecureWay User Administration Gateway Package installieren
- LDAP-Pakete (Lightweight Directory Access Protocol) installieren
- Pakete für OS/2-Server und -Gateway installieren
- Pakete für AS/400-Server und -Gateway installieren
- OnePassword-Paket installieren

In den Tivoli SecureWay User Administration Release Notes finden Sie darüber hinaus Einzelangaben zu den neuesten Modulversionen und unterstützten Systemkonfigurationen sowie Informationen zur Installation und Deinstallation von Ergänzungssoftware.

Tivoli SecureWay User Administration - Installationspakete

Tivoli SecureWay User Administration setzt sich aus mehreren Softwarepaketen zusammen, die einzeln installiert werden. Die Reihenfolge, in der Tivoli SecureWay User Administration und das Gateway-Paket für Tivoli SecureWay User Administration installiert werden, spielt keine Rolle, beide müssen jedoch vor der Installation der anderen Pakete installiert werden.

Für die Installation dieser Pakete ist die Berechtigungsklasse **install_product** oder **super** erforderlich. Für eine Installation über die Tivoli-Arbeitsoberfläche benötigen Sie zusätzlich die Berechtigungsklasse **user**.

- Mit **Tivoli SecureWay User Administration, Version 3.8** werden in Ihrer TME (Tivoli Management Environment) die Funktionen für die Benutzer- und Gruppenverwaltung sowie für die NIS-Verwaltung (NIS = Network Information Systems) hinzugefügt. Es muss auf dem Server und auf Tivoli-verwalteten Knoten installiert werden, die mit Tivoli SecureWay User Administration verwaltet werden sollen.

  Anmerkung: Sie müssen Tivoli SecureWay User Administration zunächst auf dem TMR-Server (TMR = Tivoli Management Region) installieren. Erst danach kann die Installation auch auf anderen Systemen in der TMR erfolgen.

- **Tivoli SecureWay User Administration Gateway Package, Version 3.8** muss auf allen Gateways in der TMR installiert werden. Bei der Verteilung an einen Endpunkt bzw. der Datenweitergabe von einem Endpunkt müssen die für den Endpunkt erforderlichen Dateien vom Gateway an den Endpunkt gesendet werden.

- **Tivoli SecureWay User Administration for LDAP Server Package, Version 3.8** sollte nur installiert werden, wenn das LDAP-Protokoll (LDAP = Lighweight Directory Access Protocol) in Ihrer Umgebung verwaltet werden soll. Dieses Paket

muss auf einer Maschine installiert werden, auf der **Tivoli SecureWay User Administration, Version 3.8** installiert wurde. Außerdem kann erst nach Installation dieses Pakets **Tivoli SecureWay User Administration Export SSL LDAP Connection, Version 3.8** installiert werden.

- **Tivoli SecureWay User Administration Export SSL LDAP Connection, Version 3.8** muss auf allen verwalteten Knoten mit einem LDAP-Anschluss installiert werden. Die beiden LDAP-Pakete können auf derselben Maschine wie der LDAP-Verzeichnisserver installiert werden, sofern die betreffende Plattform von Tivoli unterstützt wird.
- **Tivoli SecureWay User Administration for OS/2 Server Package, Version 3.8** sollte nur installiert werden, wenn Sie OS/2-Konten verwalten möchten. Dieses Paket muss auf einer Maschine installiert werden, auf der **Tivoli SecureWay User Administration, Version 3.8** installiert wurde.
- **Tivoli SecureWay User Administration for OS/2 Gateway Package, Version 3.8** muss auf allen Gateways installiert werden, die einem oder mehreren OS/2-Endpunkten zugeordnet sind. Dieses Paket muss auf einer Maschine installiert werden, auf der **Tivoli SecureWay User Administration Gateway Package, Version 3.8** installiert wurde.
- **Tivoli SecureWay User Administration for AS/400 Server Package, Version 3.8** sollte nur installiert werden, wenn es für die Verwaltung von AS/400- Konten erforderlich ist. Dieses Paket muss auf einer Maschine installiert werden, auf der **Tivoli SecureWay User Administration, Version 3.8** installiert wurde.
- **Tivoli SecureWay User Administration for AS/400 Gateway Package, Version 3.8** muss auf allen Gateways installiert werden, die einem oder mehreren AS/400-Endpunkten zugeordnet sind. Dieses Paket muss auf einer Maschine installiert werden, auf der **Tivoli SecureWay User Administration Gateway Package, Version 3.8** installiert wurde.
- **Tivoli SecureWay User Administration OnePassword, Version 3.8** sollte installiert werden, wenn die Benutzer und Administratoren über einen Web-Browser die Benutzerkennwörter in der

TME-Datenbank ändern und die aktualisierten Kennwörter an die zugeordneten Endpunkte verteilen können sollen. Dieses Paket muss auf einer Maschine installiert werden, auf der **Tivoli SecureWay User Administration, Version 3.8** installiert wurde. Außerdem muss auf der Maschine ein SSL-fähiger Webserver installiert sein.

Anmerkung: **Tivoli SecureWay 3.8 Toolkit Package** ist im Lieferumfang von Tivoli SecureWay User Administration 3.8 enthalten. Anweisungen zur Installation des Toolkit-Pakets können Sie dem Handbuch *Tivoli SecureWay Application Management Toolkit Guide* entnehmen.

Darüber hinaus muss der Befehl **wpasswd** auf einem Endpunkt installiert werden, damit er auf diesem Endpunkt verwendet werden kann. Weitere Informationen finden Sie unter „Befehl 'wpasswd' installieren" auf Seite 69

Vor der Installation der Pakete von Tivoli SecureWay User Administration sollten Sie zunächst folgende Abschnitte lesen:

- Softwarevoraussetzungen
- Hardwarevoraussetzungen

Lesen Sie zusätzlich die *Tivoli SecureWay User Administration Release Notes*. Die Release-Notes enthalten mögliche Änderungen am Installationsverfahren sowie Lösungen für bekannte Probleme.

Softwarevoraussetzungen

Die folgende Software muss vor der Installation von Tivoli SecureWay User Administration 3.8 installiert und aktiv sein:

- Tivoli Management Framework, Version 3.7B oder 3.7.1

In den *Tivoli SecureWay User Administration Release Notes* werden plattformspezifische Programmkorrekturen (Patches) aufgelistet, die vor der Installation der Software von Tivoli SecureWay User Administration installiert werden müssen.

Hardwarevoraussetzungen

Hinweise zum Plattenspeicherbedarf der Software auf Clients und Servern finden Sie in den *Tivoli SecureWay User Administration Release Notes*.

Anmerkungen vor der Softwareinstallation

Die Beachtung der folgenden Punkte vor der Installation von Tivoli SecureWay User Administration Version 3.8 kann nach der Installation wertvolle Zeit sparen.

- Stellen Sie vor der Installation von Tivoli SecureWay User Administration Version 3.8 sicher, dass ausreichend Speicherplatz in Ihrem Verzeichnis verfügbar ist. Dies ist besonders bei der Installation auf einem UNIX-System wichtig.
- Installieren Sie die verwalteten Knoten vor der Installation von Tivoli SecureWay User Administration. Dadurch werden alle verwalteten Knoten bei der Installation automatisch aktualisiert; andernfalls muss die Aktualisierung später erfolgen.
- Wie viele Produkte sollen installiert werden? Soll nur eines installiert werden, klicken Sie zur Ausführung der Installation auf **Installieren und schließen**. Sollen mehrere Produkte installiert werden, klicken Sie auf **Installieren**, um nach Installation des zuvor ausgewählten Produkts in den Dialog **Produkt installieren** zurückzukehren.
- Schließen Sie vor der Installation von Aktualisierungen von Tivoli SecureWay User Administration Version 3.8 bzw. von Erweiterungsprodukten zunächst alle Benutzer- und Gruppenprofildialoge. Andernfalls kann es zu einem Fehler in der Transaktionssperre kommen, und die Installation schlägt unter Umständen fehl.
- Die Anwendung Tivoli SecureWay User Administration stellt in Ihrer TME (Tivoli Management Environment) die Funktionen für die Benutzer- und Gruppenverwaltung sowie für die NIS-Verwaltung (NIS = Network Information Systems) zur Verfügung. In diesem Kapitel erhalten Sie die erforderlichen Informationen für die Installation dieser Anwendung.

- Wenn Sie Tivoli SecureWay User Administration installieren, fügen Sie Ihrer Tivoli-Installation die Möglichkeit zur Benutzer-, Gruppen- und NIS-Verwaltung hinzu. Diese Anwendung kann als Server oder verwalteter Knoten unter AIX, HP-UX, Solaris oder Windows NT laufen.

Mit Tivoli Software Installation Service installieren

SIS (Software Installation Service) können mehrere Tivoli-Produkte auf mehreren Systemen parallel installiert werden. Dieses auf Java basierende Produkt kann daher mehr Produkte auf mehr Systemen in sehr viel weniger Zeit installieren als die Installationsfunktion von Framework. SIS prüft, ob die Produktvoraussetzungen und, sofern definiert, die benutzerdefinierten Voraussetzungen erfüllt sind, und stellt so sicher, dass möglichst wenige Installationen fehlschlagen. Fehler bei der Installation treten normalerweise nur dann auf, wenn Maschinen ausgeschaltet oder aus dem Netzwerk entfernt werden.

SIS erstellt außerdem ein ***Installations-Repository*** (IR), in das Sie das Installationsimage eines oder mehrerer Tivoli-Produkte importieren können. Sie können nur die für die Umgebung erforderlichen Interpreter-Arten (Betriebssystemarten) importieren, wodurch Plattenspeicherplatz gespart und die Verarbeitungszeit verkürzt wird. Das IR wird dann die Quelle für alle Tivoli-Installationen. Sie können sogar ein einziges IR über mehrere TMRs hinweg gemeinsam benutzen.

Anweisungen zum Installieren von SIS in Ihrer Tivoli-Umgebung und zur Installation anderer Produkte mit SIS finden Sie im Handbuch *Tivoli Software Installation Service User's Guide*.

Tivoli SecureWay User Administration installieren

Sie können die Anwendung Tivoli SecureWay User Administration über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile installieren. Wiederholen Sie diese Installationsanweisungen für jeden Tivoli-Bereich, der mit Tivoli SecureWay User Administration verwaltet werden soll.

Vor und nach der Installation einer Anwendung sollten Sie Ihre Tivoli-Datenbank sichern. Ergibt sich bei der Installation einer Anwendung ein Problem, können Sie hierdurch Ihre Datenbank auf den Stand vor der Installation zurücksetzen. Wählen Sie auf der Tivoli-Arbeitsoberfläche die Option **Sicherung** aus, um eine Sicherung der von Tivoli verwalteten Knoten und Server vorzunehmen. Verwenden Sie den Befehl **wbkupdb**, wenn die Sicherung von der Befehlszeile aus ausgeführt werden soll. Weitere Informationen finden Sie im Handbuch *Tivoli Management Framework Planung und Installation*.

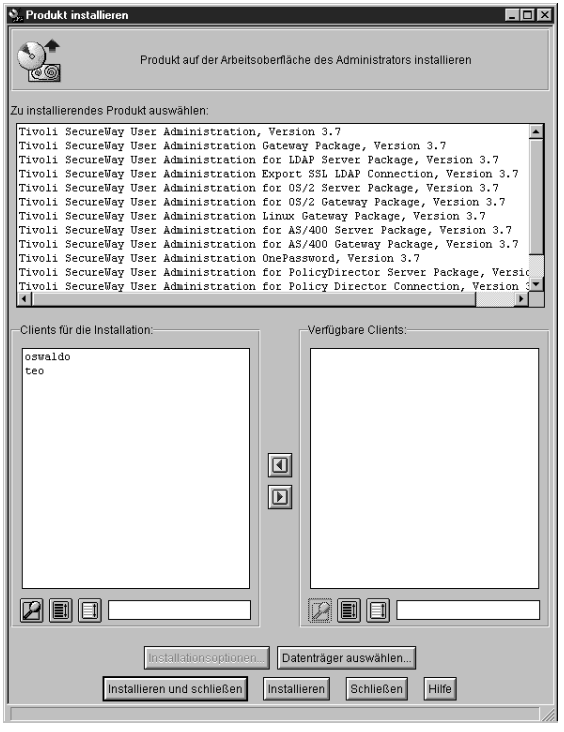
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklassen, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklassen
Tivoli SecureWay User Administration installieren	TMR	**install_product** oder **super**

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um die Anwendung Tivoli SecureWay User Administration über die Tivoli-Arbeitsoberfläche zu installieren:

1. Wählen Sie im Menü **Arbeitsoberfläche** die Option **Installieren –> Produkt installieren** aus, um den Dialog **Produkt installieren** anzuzeigen.


Produkt installieren
Produkt auf der Arbeitsoberfläche des Administrators installieren
Zu installierendes Produkt auswählen:
Tivoli SecureWay User Administration, Version 3.7
Tivoli SecureWay User Administration Gateway Package, Version 3.7
Tivoli SecureWay User Administration for LDAP Server Package, Version 3.7
Tivoli SecureWay User Administration Export SSL LDAP Connection, Version 3.7
Tivoli SecureWay User Administration for OS/2 Server Package, Version 3.7
Tivoli SecureWay User Administration for OS/2 Gateway Package, Version 3.7
Tivoli SecureWay User Administration Linux Gateway Package, Version 3.7
Tivoli SecureWay User Administration for AS/400 Server Package, Version 3.7
Tivoli SecureWay User Administration for AS/400 Gateway Package, Version 3.7
Tivoli SecureWay User Administration OnePassword, Version 3.7
Tivoli SecureWay User Administration for PolicyDirector Server Package, Versio
Tivoli SecureWay User Administration for Policy Director Connection, Version 3
Clients für die Installation:
oswaldo
teo
Verfügbare Clients:
Installationsoptionen...
Datenträger auswählen...
Installieren und schließen
Installieren
Schließen
Hilfe

- Wenn **Tivoli SecureWay User Administration, Version 3.8** nicht in der Liste **Zu installierendes Produkt auswählen** enthalten ist, fahren Sie mit Schritt 2 fort.
- Wenn **Tivoli SecureWay User Administration, Version 3.8** in der Liste enthalten ist, fahren Sie mit Schritt 4 fort.

2. Klicken Sie auf **Datenträger auswählen**, um den Dialog **Datei-Browser** anzuzeigen.

Mit dem Dialog **Datei-Browser** können Sie den Pfad zum Installationsdatenträger angeben.

a. Geben Sie den vollständigen Pfad in das Feld **Pfadname** ein.

b. Klicken Sie auf **Pfad festlegen**, um das angegebene Verzeichnis zu ändern.

c. Klicken Sie auf **Datenträger festlegen und schließen**, um den neuen Datenträgerpfad zu speichern und zum Dialog **Produkt installieren** zurückzukehren. Der Dialog enthält nun eine Liste der für die Installation verfügbaren Produkte.

3. Gehen Sie wie folgt vor, wenn Sie den genauen Pfad zum CD-ROM-Image nicht kennen:

a. Wählen Sie in der Liste **Hosts** den Host aus, an den der Installationsdatenträger angehängt ist. Durch die Auswahl eines Hosts wird die Liste **Verzeichnisse** so aktualisiert, dass die Verzeichnisse des ausgewählten Hosts angezeigt werden.

b. Wählen Sie in der Liste **Verzeichnisse** das Verzeichnis mit dem Installationsdatenträger aus.

c. Klicken Sie auf **Datenträger festlegen und schließen**, um den neuen Datenträgerpfad zu speichern und zum Dialog **Produkt installieren** zurückzukehren. Der Dialog enthält nun eine Liste der für die Installation verfügbaren Produkte.

4. Wählen Sie **Tivoli SecureWay User Administration, Version 3.8** in der Liste **Zu installierendes Produkt auswählen** aus.

5. Verwenden Sie zur Angabe der Clients, auf denen dieses Produkt installiert werden soll, die Pfeiltasten, um Clientnamen zwischen der Liste **Clients für die Installation** und der Liste **Verfügbare Clients** zu verschieben. Standardmäßig sind alle Clients in der aktuellen TMR in der Liste **Clients für die Installation** enthalten.

6. Klicken Sie auf **Installieren und schließen**, wenn nur ein Produkt installiert werden soll. Sollen mehrere Produkte installiert werden, klicken Sie auf **Installieren**, um in den Dialog **Produkt installieren** zurückzukehren.

   Der Installationsprozess zeigt nun einen Produktinstallationsdialog an. In diesem Dialog wird die Liste der Vorgänge angezeigt, die während des Installationsprozesses ausgeführt werden. Außerdem werden Sie in diesem Dialog auf Probleme aufmerksam gemacht, die vor der Installation der Anwendung korrigiert werden sollten.

7. Wählen Sie **Installieren** aus, um mit dem Installationsprozess zu beginnen und den Dialog mit dem Status der Produktinstallation anzuzeigen. Der Dialog **Produkt installieren** enthält Statusinformationen zur Installation.

   Wenn die Installation beendet ist, wird im Produktinstallationsdialog eine Abschlussnachricht zurückgegeben.

8. Klicken Sie auf **Schließen**, um den Dialog zu schließen. Tivoli SecureWay User Administration ist nun auf den ausgewählten verwalteten Knoten installiert.

Befehlszeile

Im folgenden Beispiel wird Tivoli SecureWay User Administration Version 3.8 installiert:

```
winstall -c /cdrom -s graceland -i ADMIN.IND
```

Dabei gilt Folgendes:

-c /cdrom	Gibt den Pfad zum CD-ROM-Image an.
-s graceland	Gibt **graceland** als TMR-Server an.
-i ADMIN.IND	Gibt die Indexdatei an, über die Tivoli SecureWay User Administration installiert wird.

Weitere Informationen finden Sie im Abschnitt zum Befehl **winstall** im Handbuch *Tivoli Framework Reference Manual*.

Tivoli SecureWay User Administration Gateway Package installieren

Die Gateway-Software läuft auf verwalteten Knoten und ermöglicht so deren Einsatz als Gateway zwischen einem Endpunktverbund und der restlichen Tivoli-Umgebung. Über Gateways können Endpunkte ausführbare Dateien in einen Cache herunterladen und ausführen, ohne dass hierzu lokale Datenbanken erforderlich sind. Jeder TMR können mehrere (oder keine) Gateways zugeordnet sein.

Das Tivoli SecureWay User Administration Gateway Package muss auf allen Gateways mit Endpunkten, die mit Tivoli SecureWay User Administration verwaltet werden sollen, installiert werden. Für Endpunkte ist es erforderlich, dass die Gateway-Software auf dem Gateway installiert ist, dem die Endpunkte zugeordnet sind.

Nehmen wir einmal folgende Konfiguration an:

- Das Gateway **GW1** ist auf dem verwalteten Knoten **fuji** installiert.
- Der Endpunkt **eep** ist an **GW1** angemeldet.

- **eep** ist Subskribent des Profilmanagers mit dem Benutzerprofil UP1.

In dieser Konfiguration muss das Tivoli SecureWay User Administration Gateway Package auf **fuji** installiert werden, damit eine erfolgreiche Verteilung des Benutzerprofils UP1 an **eep** möglich ist.

Wird das Gateway-Paket nicht auf der für einen bestimmten Endpunkt erforderlichen Maschine installiert, wird bei der versuchten Ausführung einer Tivoli SecureWay User Administration-Funktion auf diesem Endpunkt eine Nachricht wie diese ausgegeben:

```
UP1: Distribute failed for subscriber 'eep':
->1999-01-18 17:59:53 (4): resource
`e:/installs/Tivoli/usr/bin/lcf_bundle//bin/w32-ix86/TME/
USERMANAGEMENT/umbo_skel1' not found.
```

Sie können Tivoli SecureWay User Administration Gateway Package Version 3.8 über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile installieren.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um das Tivoli SecureWay User Administration Gateway Package über die Tivoli-Arbeitsoberfläche zu installieren:

1. Wählen Sie im Menü **Arbeitsoberfläche** die Option **Installieren –> Produkt installieren** aus, um den Dialog **Produkt installieren** anzuzeigen.
2. Wählen Sie **Tivoli SecureWay User Administration Gateway Package, Version 3.8** in der Liste **Zu installierendes Produkt auswählen** aus.
3. Verwenden Sie zur Angabe der Gateways, auf denen dieses Produkt installiert werden soll, die Pfeiltasten, um Clientnamen zwischen der Liste **Clients für die Installation** und der Liste **Verfügbare Clients** zu verschieben. Standardmäßig sind alle Clients in der aktuellen TMR in der Liste **Clients für die Installation** enthalten.

4. Klicken Sie auf **Installieren und schließen**, wenn nur ein Produkt installiert werden soll. Sollen mehrere Produkte installiert werden, klicken Sie auf **Installieren**, um in den Dialog **Produkt installieren** zurückzukehren.

   Der Installationsprozess zeigt nun einen Produktinstallationsdialog an. In diesem Dialog wird die Liste der Vorgänge angezeigt, die während des Installationsprozesses ausgeführt werden. Außerdem werden Sie in diesem Dialog auf Probleme aufmerksam gemacht, die vor der Installation der Anwendung korrigiert werden sollten.

5. Wählen Sie **Installieren** aus, um mit dem Installationsprozess zu beginnen und den Dialog mit dem Status der Produktinstallation anzuzeigen. Der Dialog **Produkt installieren** enthält Statusinformationen zur Installation.

   Wenn die Installation beendet ist, wird im Produktinstallationsdialog eine Abschlussnachricht zurückgegeben.

6. Klicken Sie auf **Schließen**, um den Dialog zu schließen. Tivoli SecureWay User Administration ist nun auf den ausgewählten verwalteten Knoten installiert.

Befehlszeile

Im folgenden Beispiel wird das Tivoli SecureWay User Administration Gateway Package installiert.

```
winstall -c /cdrom -s fuji -i ADMIN_GW.IND
```

Dabei gilt Folgendes:

-c /cdrom	Gibt den Pfad zum CD-ROM-Image an.
-s fuji	Gibt an, dass der verwaltete Knoten **fuji** als Gateway eingesetzt wird.
-i ADMIN_GW.IND	Gibt die Indexdatei an, über die das Tivoli SecureWay User Administration Gateway Package installiert wird.

Weitere Informationen finden Sie im Abschnitt zum Befehl **winstall** im Handbuch *Tivoli Framework Reference Manual*.

LDAP-Pakete installieren

Das Tivoli SecureWay User Administration for LDAP Server Package sollte nur installiert werden, wenn das LDAP-Protokoll (LDAP = Lighweight Directory Access Protocol) in Ihrer Umgebung verwaltet werden soll. Dieses Paket muss auf einer Maschine mit Tivoli SecureWay User Administration installiert werden.

Tivoli SecureWay User Administration Export SSL LDAP Connection muss auf allen verwalteten Knoten mit einem LDAP-Anschluss installiert werden. Die beiden LDAP-Pakete können auf derselben Maschine wie der LDAP-Verzeichnisserver installiert werden, sofern die betreffende Plattform von Tivoli unterstützt wird.

Anmerkung: Vor der Installation des Pakets **Export SSL LDAP Connection** müssen Sie zunächst die LDAP-Serversoftware installieren.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um das LDAP-Paket über die Tivoli-Arbeitsoberfläche zu installieren:

1. Wählen Sie im Menü **Arbeitsoberfläche** die Option **Installieren –> Produkt installieren** aus, um den Dialog **Produkt installieren** anzuzeigen.
2. Wählen Sie in der Liste **Zu installierendes Produkt auswählen** die Option **Tivoli SecureWay User Administration for LDAP Server Package, Version 3.8** oder **Tivoli SecureWay User Administration Export SSL LDAP Connection, Version 3.8** aus.
3. Verwenden Sie zur Angabe der Maschinen, auf denen dieses Produkt installiert werden soll, die Pfeiltasten, um Clientnamen zwischen der Liste **Clients für die Installation** und der Liste **Verfügbare Clients** zu verschieben. Standardmäßig sind alle Clients in der aktuellen TMR in der Liste **Clients für die Installation** enthalten.

Folgendes sollten Sie bei der Auswahl der Maschinen, auf denen die LDAP-Pakete installiert werden sollen, beachten:

- **Tivoli SecureWay User Administration for LDAP Server Package, Version 3.8** muss auf einer Maschine mit **Tivoli SecureWay User Administration, Version 3.8** installiert werden.
- Installieren Sie **Tivoli SecureWay User Administration Export SSL LDAP Connection, Version 3.8** auf allen verwalteten Knoten mit einem LDAP-Anschluss.

Die beiden LDAP-Pakete können auf derselben Maschine wie der LDAP-Verzeichnisserver installiert werden, sofern die betreffende Plattform von Tivoli unterstützt wird.

4. Klicken Sie auf **Installieren und schließen**, wenn nur ein Produkt installiert werden soll. Sollen mehrere Produkte installiert werden, klicken Sie auf **Installieren**, um in den Dialog **Produkt installieren** zurückzukehren.

   Der Installationsprozess zeigt nun einen Produktinstallationsdialog an. In diesem Dialog wird die Liste der Vorgänge angezeigt, die während des Installationsprozesses ausgeführt werden. Außerdem werden Sie in diesem Dialog auf Probleme aufmerksam gemacht, die vor der Installation der Anwendung korrigiert werden sollten.

5. Wählen Sie **Installieren** aus, um mit dem Installationsprozess zu beginnen und den Dialog mit dem Status der Produktinstallation anzuzeigen. Der Dialog **Produkt installieren** enthält Statusinformationen zur Installation.

   Wenn die Installation beendet ist, wird im Produktinstallationsdialog eine Abschlussnachricht zurückgegeben.

6. Klicken Sie auf **Schließen**, um den Dialog zu schließen. Tivoli SecureWay User Administration ist nun auf den ausgewählten verwalteten Knoten installiert.

Befehlszeile

Im folgenden Beispiel wird Tivoli SecureWay User Administration for LDAP Server Package installiert:

```
winstall -c /cdrom -s graceland -i ALDAPEXT.IND
```

Dabei gilt Folgendes:

-c /cdrom Gibt den Pfad zum CD-ROM-Image an.

-s graceland Gibt an, dass der verwaltete Knoten **graceland** der Installationsserver ist. Tivoli SecureWay User Administration ist auf dieser Maschine bereits installiert.

-i ALDAPEXT.IND
Gibt die Indexdatei an, über die Tivoli SecureWay User Administration for LDAP Server Package installiert wird.

Im folgenden Beispiel wird Tivoli SecureWay User Administration Export SSL LDAP Connection installiert:

```
winstall -c /cdrom -s graceland -i ALDAPCON.IND
```

Dabei gilt Folgendes:

-c /cdrom Gibt den Pfad zum CD-ROM-Image an.

-s graceland Gibt an, dass der verwaltete Knoten **graceland** der Installationsserver ist. Tivoli SecureWay User Administration ist auf dieser Maschine bereits installiert.

-i ALDAPCON.IND
Gibt die Indexdatei an, über die Tivoli SecureWay User Administration Export SSL LDAP Connection installiert wird.

Weitere Informationen finden Sie im Abschnitt zum Befehl **winstall** im Handbuch *Tivoli Framework Reference Manual*.

OS/2-Pakete installieren

Tivoli SecureWay User Administration for OS/2 kann zusammen mit Tivoli SecureWay User Administration für die Verwaltung von Benutzerkonten unter OS/2 Warp eingesetzt werden. Für alle Benutzerinformationen, die über die grafische OS/2-Benutzerschnittstelle verwaltet werden können, ist auch eine Verwaltung über Tivoli SecureWay User Administration for OS/2 möglich.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um das OS/2-Paket über die Tivoli-Arbeitsoberfläche zu installieren:

1. Wählen Sie im Menü **Arbeitsoberfläche** die Option **Installieren –> Produkt installieren** aus, um den Dialog **Produkt installieren** anzuzeigen.
2. Wählen Sie in der Liste **Zu installierendes Produkt auswählen** die Option **Tivoli SecureWay User Administration for OS/2 Server Package, Version 3.8** oder **Tivoli SecureWay User Administration for OS/2 Gateway Package, Version 3.8** aus.
3. Verwenden Sie zur Angabe der Maschinen, auf denen dieses Produkt installiert werden soll, die Pfeiltasten, um Clientnamen zwischen der Liste **Clients für die Installation** und der Liste **Verfügbare Clients** zu verschieben. Standardmäßig sind alle Clients in der aktuellen TMR in der Liste **Clients für die Installation** enthalten.

   Folgendes sollten Sie bei der Auswahl der Maschinen, auf denen die OS/-Pakete installiert werden sollen, beachten:

   - **Tivoli SecureWay User Administration for OS/2 Server Package, Version 3.8** darf nur auf Maschinen installiert werden, auf denen **Tivoli SecureWay User Administration, Version 3.8** installiert ist.
   - **Tivoli SecureWay User Administration for OS/2 Gateway Package, Version 3.8** darf nur auf Maschinen installiert werden, auf denen **Tivoli SecureWay User Administration Gateway Package, Version 3.8** installiert ist.

4. Klicken Sie auf **Installieren und schließen**, wenn nur ein Produkt installiert werden soll. Sollen mehrere Produkte installiert werden, klicken Sie auf **Installieren**, um in den Dialog **Produkt installieren** zurückzukehren.

   Der Installationsprozess zeigt nun einen Produktinstallationsdialog an. In diesem Dialog wird die Liste der Vorgänge angezeigt, die während des Installationsprozesses ausgeführt werden. Außerdem werden Sie in diesem Dialog auf Probleme aufmerksam gemacht, die vor der Installation der Anwendung korrigiert werden sollten.

5. Wählen Sie **Installieren** aus, um mit dem Installationsprozess zu beginnen und den Dialog mit dem Status der Produktinstallation anzuzeigen. Der Dialog **Produkt installieren** enthält Statusinformationen zur Installation.

   Wenn die Installation beendet ist, wird im Produktinstallationsdialog eine Abschlussnachricht zurückgegeben.

6. Klicken Sie auf **Schließen**, um den Dialog zu schließen. Tivoli SecureWay User Administration ist nun auf den ausgewählten verwalteten Knoten installiert.

Befehlszeile

Im folgenden Beispiel wird das Tivoli SecureWay User Administration for OS/2 Server Package installiert:

```
winstall -c /cdrom -s graceland -i OS2.IND
```

Dabei gilt Folgendes:

-c /cdrom	Gibt den Pfad zum CD-ROM-Image an.
-s graceland	Gibt an, dass das Paket auf dem verwalteten Knoten **graceland** installiert wird. Tivoli SecureWay User Administration ist auf dieser Maschine bereits installiert.

-i OS2.IND	Gibt die Indexdatei an, über die das Tivoli SecureWay User Administration for OS/2 Server Package installiert wird.

Im folgenden Beispiel wird das Tivoli SecureWay User Administration for OS/2 Gateway Package installiert:

```
winstall -c /cdrom -s fuji -i OS2GW.IND
```

Dabei gilt Folgendes:

-c /cdrom	Gibt den Pfad zum CD-ROM-Image an.
-s fuji	Gibt an, dass das Paket auf dem Gateway **fuji** installiert wird. Das Tivoli SecureWay User Administration Gateway Package ist auf dieser Maschine bereits installiert.
-i OS2GW.IND	Gibt die Indexdatei an, über die das Tivoli SecureWay User Administration for OS/2 Gateway Package installiert wird.

Weitere Informationen finden Sie im Abschnitt zum Befehl **winstall** im Handbuch *Tivoli Framework Reference Manual*.

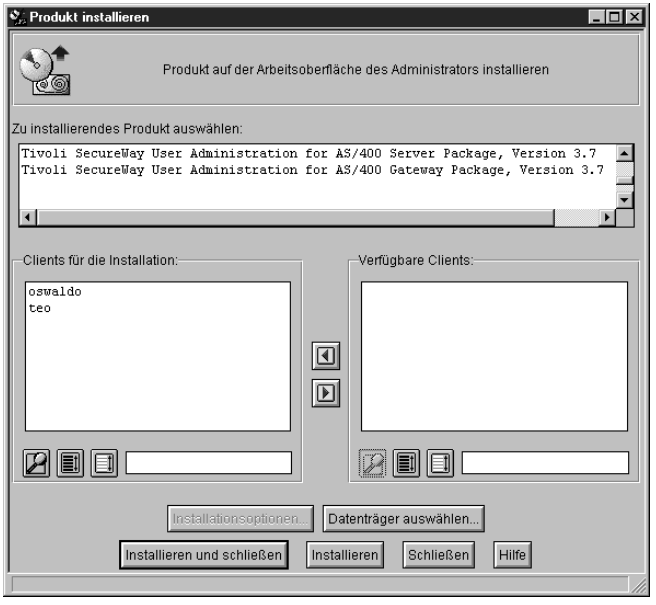
AS/400-Pakete installieren

Tivoli SecureWay User Administration for AS/400 kann zusammen mit Tivoli SecureWay User Administration für die Verwaltung von Benutzerkonten unter AS/400 eingesetzt werden. Weitere Informationen zur Verwaltung von AS/400-Konten finden Sie im AS/400-Anhang des Handbuchs *Tivoli SecureWay User Administration Management Handbuch*.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um das AS/400-Paket über die Tivoli-Arbeitsoberfläche zu installieren:

1. Wählen Sie im Menü **Arbeitsoberfläche** die Option **Installieren –> Produkt installieren** aus, um den Dialog **Produkt installieren** anzuzeigen.



2. Wählen Sie in der Liste **Zu installierendes Produkt auswählen** die Option **Tivoli SecureWay User Administration for AS/400 Server Package, Version 3.8** oder **Tivoli SecureWay User Administration for AS/400 Gateway Package, Version 3.8** aus.

3. Verwenden Sie zur Angabe der Maschinen, auf denen dieses Produkt installiert werden soll, die Pfeiltasten, um Clientnamen zwischen der Liste **Clients für die Installation** und der Liste **Verfügbare Clients** zu verschieben. Standardmäßig sind alle Clients in der aktuellen TMR in der Liste **Clients für die Installation** enthalten.

Folgendes sollten Sie bei der Auswahl der Maschinen, auf denen die AS/400-Pakete installiert werden sollen, beachten:

- **Tivoli SecureWay User Administration for AS/400 Server Package, Version 3.8** darf nurauf Maschinen installiert werden, auf denen **Tivoli SecureWay User Administration, Version 3.8** installiert ist.
- **Tivoli SecureWay User Administration for AS/400 Gateway Package, Version 3.8** darf nur auf Maschinen installiert werden, auf denen **Tivoli SecureWay User Administration Gateway Package, Version 3.8** installiert ist.

4. Klicken Sie auf **Installieren und schließen**, wenn nur ein Produkt installiert werden soll. Sollen mehrere Produkte installiert werden, klicken Sie auf **Installieren**, um in den Dialog **Produkt installieren** zurückzukehren.

   Der Installationsprozess zeigt nun einen Produktinstallationsdialog an. In diesem Dialog wird die Liste der Vorgänge angezeigt, die während des Installationsprozesses ausgeführt werden. Außerdem werden Sie in diesem Dialog auf Probleme aufmerksam gemacht, die vor der Installation der Anwendung korrigiert werden sollten.

5. Wählen Sie **Installieren** aus, um mit dem Installationsprozess zu beginnen und den Dialog mit dem Status der Produktinstallation anzuzeigen. Der Dialog **Produkt installieren** enthält Statusinformationen zur Installation.

   Wenn die Installation beendet ist, wird im Produktinstallationsdialog eine Abschlussnachricht zurückgegeben.

6. Klicken Sie auf **Schließen**, um den Dialog zu schließen. Tivoli SecureWay User Administration ist nun auf den ausgewählten verwalteten Knoten installiert.

Befehlszeile

Im folgenden Beispiel wird das Tivoli SecureWay User Administration for AS/400 Server Packageinstalliert:

```
winstall -c /cdrom -s graceland -i OS4.IND
```

Dabei gilt Folgendes:

-c /cdrom Gibt den Pfad zum CD-ROM-Image an.

-s graceland Gibt an, dass das Paket auf dem verwalteten Knoten **graceland** installiert wird. Tivoli SecureWay User Administration ist auf dieser Maschine bereits installiert.

-i OS4.IND Gibt die Indexdatei an, über die das Tivoli SecureWay User Administration for AS/400 Server Package installiert wird.

Im folgenden Beispiel wird das Tivoli SecureWay User Administration for AS/400 Gateway Package installiert:

```
winstall -c /cdrom -s fuji -i OS4GW.IND
```

Dabei gilt Folgendes:

-c /cdrom Gibt den Pfad zum CD-ROM-Image an.

-s fuji Gibt an, dass das Paket auf dem Gateway **fuji** installiert wird. Das Tivoli SecureWay User Administration Gateway Package ist auf dieser Maschine bereits installiert.

-i OS4GW.IND
Gibt die Indexdatei an, über die das Tivoli SecureWay User Administration for AS/400 Gateway Package installiert wird.

Weitere Informationen finden Sie im Abschnitt zum Befehl **winstall** im Handbuch *Tivoli Framework Reference Manual*.

OnePassword-Paket installieren

Tivoli SecureWay User Administration OnePassword ermöglicht Benutzern und Administratoren das Ändern von Benutzerkennwörtern in der TME-Datenbank sowie die Verteilung der aktualisierten Kennwörter an die zugeordneten Endpunkte. Dies geschieht über einen Web-Browser. Eine Sicherung der TME-Datenbank wird sowohl vor als auch nach der Installation von OnePassword empfohlen, damit Sie die ursprüngliche Datenbank wiederherstellen können, falls sich während der Installation von OnePassword ein Problem ergibt.

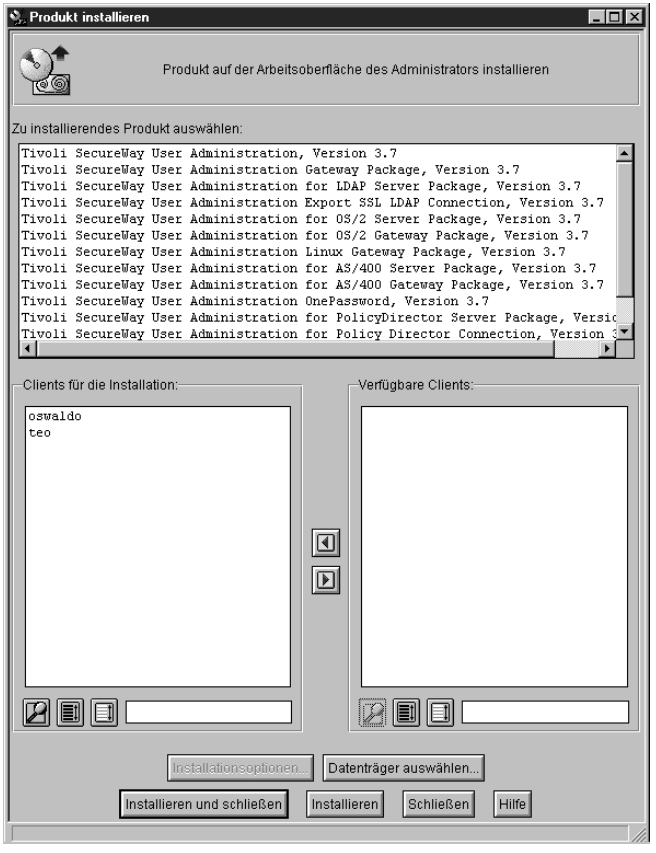
Anmerkung: Die Installation von OnePassword erfolgt in zwei Schritten. Der erste in diesem Abschnitt beschriebene Schritt umfasst die Installation der Image-Dateien in die entsprechenden Verzeichnisse des TMR-Servers. Im zweiten Schritt (beschrieben unter „Befehl 'wonepassinst' ausführen" auf Seite 67) werden diese Images in die Verzeichnisse des Webservers auf derselben Maschine installiert.

Der Webserver **muss** auf derselben Maschine wie der TMR-Server installiert werden. Der Webserver sollte möglichst SSL-fähig sein. Wenn Sie den Webserver nicht auf derselben Maschine installieren, kann OnePassword weder installiert noch verwendet werde.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um OnePassword über die Tivoli-Arbeitsoberfläche zu installieren:

1. Wählen Sie im Menü **Arbeitsoberfläche** die Option **Installieren –> Produkt installieren** aus, um den Dialog **Produkt installieren** anzuzeigen.


Produkt installieren
Produkt auf der Arbeitsoberfläche des Administrators installieren
Zu installierendes Produkt auswählen:
Tivoli SecureWay User Administration, Version 3.7
Tivoli SecureWay User Administration Gateway Package, Version 3.7
Tivoli SecureWay User Administration for LDAP Server Package, Version 3.7
Tivoli SecureWay User Administration Export SSL LDAP Connection, Version 3.7
Tivoli SecureWay User Administration for OS/2 Server Package, Version 3.7
Tivoli SecureWay User Administration for OS/2 Gateway Package, Version 3.7
Tivoli SecureWay User Administration Linux Gateway Package, Version 3.7
Tivoli SecureWay User Administration for AS/400 Server Package, Version 3.7
Tivoli SecureWay User Administration for AS/400 Gateway Package, Version 3.7
Tivoli SecureWay User Administration OnePassword, Version 3.7
Tivoli SecureWay User Administration for PolicyDirector Server Package, Versic
Tivoli SecureWay User Administration for Policy Director Connection, Version 3
Clients für die Installation:
oswaldo
teo
Verfügbare Clients:
Installationsoptionen...
Datenträger auswählen...
Installieren und schließen
Installieren
Schließen
Hilfe

2. Wählen Sie **OnePassword** in der Liste **Zu installierendes Produkt auswählen** aus.

3. Verwenden Sie zur Angabe des TMR-Servers, auf dem dieses Produkt installiert werden soll, die Pfeiltasten, um den Hostnamen des TMR-Servers zwischen der Liste **Clients für die Installation** und der Liste **Verfügbare Clients** zu verschieben.

4. Klicken Sie auf **Installieren und schließen**, um das Produkt zu installieren und den Dialog **Produkt installieren** zu schließen.

   Der Installationsprozess zeigt nun einen Produktinstallationsdialog an. In diesem Dialog wird die Liste der Vorgänge angezeigt, die während des Installationsprozesses ausgeführt werden.

Außerdem werden Sie in diesem Dialog auf Probleme aufmerksam gemacht, die vor der Installation der Anwendung korrigiert werden sollten.

5. Wählen Sie **Installieren** aus, um mit dem Installationsprozess zu beginnen und den Dialog mit dem Status der Produktinstallation anzuzeigen. Der Dialog **Produkt installieren** enthält Statusinformationen zur Installation.

   Wenn die Installation beendet ist, wird im Produktinstallationsdialog eine Abschlussnachricht zurückgegeben.

6. Klicken Sie auf **Schließen**, um den Dialog zu schließen. OnePassword ist nun auf den ausgewählten verwalteten Knoten installiert.

Befehlszeile

Im folgenden Beispiel wird OnePassword installiert:

```
winstall -c /cdrom/tivoli -s memphis -i WEBPWD
```

Dabei gilt Folgendes:

-c /cdrom/tivoli	Gibt den Pfad zum CD-ROM-Image an.
-s memphis	Installiert das Paket auf dem TMR-Server **memphis**. Tivoli SecureWay User Administration ist auf dieser Maschine bereits installiert.
-i WEBPWD	Gibt die Indexdatei an, über die OnePassword installiert wird.

Befehl 'wonepassinst' ausführen

Nach der Installation der Installationsimages von OnePassword in die Verzeichnisse des TMR-Servers müssen Sie auf dem TMR-Server den Befehl **wonepassinst** ausführen, damit folgende Schritte ausgeführt werden:

- Suchen Sie die HTML-Seiten von OnePassword unter Verwendung von Nachrichten aus dem Nachrichtenkatalog **AboutWEBPWDCatalog**.

Anmerkung: Wenn Sie ein Sprachpaket für Tivoli SecureWay User Administration installieren möchten, sollte dies vor der Ausführung des Befehls **wonepassinst** erfolgen. Hierdurch wird sichergestellt, dass die HTML-Seiten von OnePassword in der richtigen Sprache installiert werden.

- Passen Sie eine der HTML-Seiten von OnePassword an, und erstellen Sie eine Prüfliste, in der die verschiedenen Endpunktarten der TMR identifiziert werden.
- Erstellen Sie dazu Kopien von den Dateien, und legen Sie diese in den Verzeichnissen **html** und **cgi** des Webservers ab.

Nachfolgend ein Beispiel für den Befehl **wonepassinst**:

```
wonepassinst https://lgrenin1/cgi-bin \
d:/Program_Files/HTTP_Server/htdocs \
d:/Program_Files/HTTP_Server/cgi-bin \
c:/WINNT/SYSTEM32/drivers/etc/Tivoli/setup_env.sh
```

Dabei gilt Folgendes:

https://lgrenin1/cgi-bin
Gibt die URL der CGI-Dateien des Webservers an.

Anmerkung: Mit diesem Argument wird auch festgelegt, ob es sich um eine sichere (HTTPS) oder um eine nicht sichere (http) Verbindung handelt. Aufgrund der vom Browser an den Server weitergegebenen Daten wird eine sichere Verbindung (HTTPS) empfohlen.

d:/Program_Files/HTTP_Server/htdocs
Gibt den Pfad zum Verzeichnis der Webservers an, in das die HTML-Dateien von OnePassword kopiert werden sollen.

d:/Program_Files/HTTP_Server/cgi-bin
Gibt den Pfad zum Verzeichnis der Webservers an, in das die Skripts und ausführbaren Dateien von OnePassword kopiert werden sollen.

c:/WINNT/SYSTEM32/drivers/etc/Tivoli/setup_env.sh
Gibt den Pfad des Skripts 'setup_env.sh' auf dem TMR-Server an.

Zusätzliche Verwendungsmöglichkeiten von 'wonepassinst'

Führen Sie den Befehl **wonepassinst** auch aus, wenn sich die Liste der vom TMR-Server unterstützten Endpunktarten ändert. Somit wird sichergestellt, dass die Liste der Optionsfelder in OnePassword aktualisiert wird. Außerdem sollten Sie **wonepassinst** ausführen, wenn sich der Standort von **setup_env.sh** oder der Pfad des Verzeichnisses **html** bzw. **cgi** ändert.

Befehl 'wpasswd' installieren

Mit dem Befehl **wpasswd** können Administratoren Endbenutzerkennwörter sowie Kennwörter für Konten auf Maschinen, auf denen Tivoli SecureWay User Administration installiert ist, ändern.

Darüber hinaus können auch normale Benutzer mit Hilfe des Befehls **wpasswd** das eigene Kennwort ändern. Er steht jedoch nur auf Endpunkten zur Verfügung, wenn er unter Verwendung des Befehls **winstpw** auf Endpunkten installiert wurde. Eine Installation des Befehls **wpasswd** über die Arbeitsoberfläche oder SIS ist nicht möglich. Der Befehl **wuninstpw** kann nur über den Befehl **wuninstpw** wieder von Endpunkten entfernt werden.

Weitere Informationen zu den Befehlen **winstpw** und **wunistpw** finden Sie im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Tivoli SecureWay User Administration aktualisieren

Tivoli SecureWay User Administration Version 3.8 und Tivoli SecureWay User Administration Gateway Package Version 3.8 können als Aktualisierungen von Tivoli SecureWay User Administration Version 3.7 installiert werden. Sie können die Pakete über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile installieren. Die erforderlichen Schritte für eine Aktualisierung von Tivoli SecureWay User Administration-Paketen sind vergleichbar mit denen für die Erstinstallation der Pakete. Im Gegensatz zur Erstinstallation wird bei der Aktualisierung jedoch nur der Code der Programmkorrektur für das Paket installiert.

Anmerkungen:

1. Stellen Sie sicher, dass Sie Ihr System sichern, bevor Sie eine Aktualisierung durchführen.
2. Wenn beim Aktualisieren neue Endpunktarten hinzugefügt werden, wird nur der Standarddatensatz in den Benutzerprofilen aktualisiert. Einzelne Benutzerdatensätze werden nicht aktualisiert. Wenn Sie Benutzerdatensätze für eine neue Endpunktart aktualisierten möchten, verwenden Sie den Befehl **wgenusrdef**. Im folgenden Beispiel werden allen Benutzerdatensätzen in “myprofile” für Windows 2000-Attribute Standardwerte hinzugefügt:

   ```
   wgenusrdef -e w2k -all @UserProfile:myprofile
   ```

Arbeitsoberfläche

Führen Sie dieselben Schritte wie bei der Installation von Tivoli SecureWay User Administration aus, jedoch mit der folgenden Ausnahme: Wählen Sie nicht, wie in den Anweisungen angegeben, die Option **Installieren –> Produkt installieren...** zur Anzeige des Dialogs **Produkt installieren** aus, sondern die Option **Installieren –> Programmkorrektur installieren...** ; hierdurch wird der Dialog **Programmkorrektur installieren** angezeigt. Wählen Sie die Programmkorrektur aus, die Sie installieren möchten, und setzen Sie den Installationsprozess fort.

Befehlszeile

Im folgenden Befehl wird das Paket für Tivoli SecureWay User Administration aktualisiert:

```
wpatch -c /cdrom graceland -i ADMINUPG
```

Dabei gilt Folgendes:

–c /cdrom	Gibt den Pfad für den Installationsdatenträger an.
graceland	Gibt den verwalteten Knoten bzw. den TMR-Server an, auf dem die vorherige Version von Tivoli SecureWay User Administration installiert ist.
–i ADMINUPG	Gibt die Indexdatei (**.IND**) an, über die die Tivoli SecureWay User Administration-Programmkorrektur installiert wird.

Mit dem folgenden Befehl wird das Tivoli SecureWay User Administration Gateway Package aktualisiert:

```
wpatch -c /cdrom fuji -i ADMGWUPG
```

Dabei gilt Folgendes:

–c /cdrom	Gibt den Pfad für den Installationsdatenträger an.
fuji	Gibt das Gateway an, auf dem die vorherige Version des Tivoli SecureWay User Administration Gateway Package installiert ist.
–i ADMGWUPG	Gibt die Indexdatei (**.IND**) an, über die die Tivoli SecureWay User Administration-Programmkorrektur installiert wird.

Tivoli SecureWay User Administration-Pakete deinstallieren

Tivoli Management Framework stellt eine Befehlszeilenfunktion zur Verfügung, mit der Module aus einem bestimmten verwalteten Knoten oder aus der gesamten TMR entfernt werden können. Der Befehl **wuninst** ist ein Wrapper-Skript, das produktspezifische Skripts zum Entfernen der Installation aufruft.

Wenn Sie den Befehl **wuninst** mit einer anwendungsspezifischen Kennung verwenden, können Sie Tivoli SecureWay User Administration-Pakete von jeder Maschine in Ihrer Umgebung oder aus der TMR entfernen. Weitere Informationen zur Befehlszeilensyntax und Verwendung des Befehls **wuninst** finden Sie im Handbuch *Tivoli Management Framework Reference Manual*.

Geben Sie die folgende Befehlszeile ein, um die Syntaxanweisung für Tivoli SecureWay User Administration anzuzeigen:

```
wuninst Kennung
```

Dabei gilt Folgendes:

Kennung
: Gibt die registrierte Produktkennung für ein Tivoli SecureWay User Administration-Modul an. Folgende Kennungen sind gültig:

Admin	Tivoli SecureWay User Administration
ADMIN_GW	Tivoli SecureWay User Administration Gateway
LDAP	Export SSL LDAP Connection
WEBPWD	OnePassword

Geben Sie beispielsweise folgenden Befehl ein, wenn Tivoli SecureWay User Administration aus der TMR entfernt werden soll, in der **graceland** als TMR-Server eingesetzt wird. Handelt es sich bei dem Knoten um den TMR-Server, wird Tivoli SecureWay User Administration vom TMR-Server und von allen verwalteten Knoten, auf denen es installiert ist, entfernt.

```
wuninst Admin graceland -rmfiles
```

Dabei gilt Folgendes:

Admin Gibt die registrierte Produktkennung für Tivoli SecureWay User Administration an.

graceland Gibt den Namen des TMR-Servers an. Da **graceland** der TMR-Server ist, wird Tivoli SecureWay User Administration von jedem verwalteten Knoten in der TMR entfernt.

–rmfiles Gibt an, dass alle lokalen Datenbankobjekte und die zugeordneten Dateien entfernt werden, unabhängig davon, ob es sich um gemeinsam genutzte Dateien handelt.

Das Standardverhalten ohne die Option **–rmfiles** ist, dass lediglich die Datenbankeinträge für den angegebenen Knoten entfernt werden. Wenn es sich bei dem Knoten um den TMR-Server handelt, werden mit dieser Option alle Datenbankobjekte entfernt.

3

Planung und Einsatz

Jeder Einsatz von Tivoli SecureWay User Administration spiegelt die einzigartigen Merkmale jeder Unternehmensumgebung wieder. Da die Struktur der Benutzerkontoinformationen für jedes Unternehmen einzigartig ist, gibt es keine Standardschablone oder “Einheitslösung” für den Einsatz von Tivoli SecureWay User Administration. Die Organisation der Benutzerkontoinformationen hängt beispielsweise davon ab, ob das Unternehmen eine zentralisierte oder dezentralisierte Struktur aufweist. Die Organisation des Personals nach Jobfunktionen, der geografischen Lage usw. kann sich ebenfalls auf die Benutzerkontoinformationen auswirken. Tivoli SecureWay User Administration ist äußerst flexibel und kann den Bedürfnissen vieler verschiedener Umgebungen angepasst werden. Sie müssen den Einsatz von Tivoli SecureWay User Administration jedoch sorgfältig planen und testen, um sicherzustellen, dass der Einsatz effektiv ist und Ihren Bedürfnissen entspricht. Dieses Kapitel enthält eine Übersicht und Erläuterungen zu diesen Themen. Detaillierte Informationen hierzu finden Sie im IBM Redbook mit dem Titel *Enterprise Security Management with Tivoli*.

Ihre Bedürfnisse hinsichtlich der Benutzerverwaltung feststellen

Für den erfolgreichen Einsatz von Tivoli SecureWay User Administration ist es notwendig, dass Sie verstehen, wie Benutzerkontoinformationen in Ihrer Umgebung strukturiert sind. Mit diesen Informationen können Sie einen Einsatzentwurf erstellen, der den entsprechenden Mitarbeitern die notwendigen Zugriffsberechtigungen für Benutzerkonten zuordnet.

In den folgenden Abschnitten finden Sie die Punkte, die Sie beachten müssen, wenn Sie Ihre Bedürfnisse für die Benutzerverwaltung feststellen.

Personen, die auf Benutzerkonten zugreifen müssen

Verschiedene Funktionsbereiche innerhalb einer Organisation müssen auf Benutzerkontoinformationen zugreifen. Diese Bedürfnisse sind je nach Organisation sehr unterschiedlich. In manchen Unternehmen werden die Benutzerkontoinformationen zentral gesteuert, so dass es nur Administratoren und nicht einmal Endbenutzern gestattet ist, Kennwörter zu ändern. In anderen Unternehmen können verschiedene Funktionsbereiche Benutzerkontoinformationen ändern. Beispielsweise können die Mitarbeiter der Personalabteilung Benutzerkontoinformationen ändern, wenn ein Mitarbeiter aus der Firma ausscheidet oder innerhalb der Firma eine andere Position übernimmt.

Es ist notwendig, dass Sie die Bedürfnisse Ihrer Organisation hinsichtlich des Zugriffs auf Benutzerkonten kennen, damit Sie die Tivoli-Berechtigungsklassen den richtigen Mitarbeitern zuordnen.

Funktionsbereiche

Die Mitarbeiter der verschiedenen Funktionsbereiche haben möglicherweise bestimmte Erwartungen, was Ihre Zugriffs- oder Steuerungsberechtigungen für Benutzerkontoinformationen anbelangt. Bei der Planung Ihres Einsatzes sollten Sie diese Bedürfnisse bzw. Erwartungen berücksichtigen. Wenn Sie Zugriffsberechtigungen für Benutzerkontoinformationen für den von Ihnen geplanten Einsatz

ändern möchten, sollten Sie die Mitarbeiter, die von diesen Änderungen betroffen sind, im Voraus informieren.

Die folgenden Funktionsbereiche benötigen oft Zugriffsberechtigungen für Benutzerkontoinformationen. Dies sind jedoch nur Beispiele. Stellen Sie sicher, dass Sie die besonderen Bedürfnisse Ihrer Umgebung berücksichtigen.

- **Systemverwaltung bzw. Informationstechnik (IT).** Normalerweise werden Benutzerkonten von Systemadministratoren eingerichtet und verwaltet.
- **Help-Desk.** Help-Desk-Mitarbeiter können Kennwörter zurücksetzen und andere Benutzerkontoinformationen ändern.
- **Personalabteilung.** Die Mitarbeiter der Personalabteilung können Benutzerkonten einrichten bzw. vorhandene Konten modifizieren, wenn Mitarbeiter Ihre Arbeitsstelle innerhalb der Firma wechseln bzw. aus der Firma ausscheiden oder wenn sie in ein anderes Büro wechseln.
- **Management.** Manager können Benutzerkonten für ihre Mitarbeiter erstellen, ändern und löschen.
- **Technische Einrichtungen.** Mitarbeiter, die für technische Einrichtungen zuständig sind, können Benutzerkontoinformationen wie beispielsweise die Bürostandorte bzw. Telefonnummern der Mitarbeiter ändern.

Berechtigungsklassen und Zuständigkeiten

Mitarbeiter, die Schlüsselpositionen einnehmen, sind für Aufgaben zuständig, die Benutzerkontoinformationen betreffen. Beispielsweise kann ein Serveradministrator bzw. ein E-Mail-Administrator Richtlinien implementieren, die die Verwaltung von Benutzerkontoinformationen betreffen.

Mitarbeiter, die für folgende Aufgaben zuständig sind, haben Einfluss auf Benutzerkontoinformationen. Überlegen Sie, ob Sie diese Personen in die Planung des Einsatzes von Tivoli SecureWay User Administration einbeziehen. Folgende Auflistung dient lediglich als Beispiel. Stellen Sie sicher, dass Sie die besonderen Bedürfnisse Ihrer Umgebung berücksichtigen.

- **Benutzer- und Gruppenadministrator.** Der Benutzer- und Gruppenadministrator ist für das Hinzufügen, Ändern, Verschieben und Löschen von angeforderten Benutzer- und Gruppenzugriffsberechtigungen für Server und andere Netzwerkressourcen zuständig. Der Benutzer- und Gruppenadministrator ist zum Beispiel für folgende Aufgaben verantwortlich:
  - Zurücksetzen des Netzwerks
  - Zurücksetzen von Benutzerkennwörtern
  - Hinzufügen, Ändern bzw. Löschen von Benutzer-IDs
  - Hinzufügen, Ändern bzw. Löschen von Gruppen
  - Verschieben von Daten (beispielsweisen das Verschieben von Dateien, die ausgeschiedene Mitarbeiter betreffen)
  - Software-Zugriff
  - Bereichszuordnungen
  - Namensänderungen
  - Zugriffsbeschränkungen für Namen
  - Berichtigungen des Anmeldeskripts
- **E-Mail-Administrator.** Der E-Mail-Administrator ist dafür verantwortlich, E-Mail-Server zu verwalten, zu installieren und zu entfernen sowie Benutzer- und Gruppenkonten für die E-Mail-Server zu verwalten. E-Mail-Administratoren sind zum Beispiel für folgende Aufgaben verantwortlich:
  - Warten und Verwalten der E-Mail-Server
  - Warten und Verwalten der Kalenderserver
  - Warten und Verwalten aller E-Mail- und Kalender-Gateways
  - Unterstützung der E-Mail-Dienste
  - Zeitgerechte Fehlerbehebung und Durchführung von Korrekturen für die verwalteten E-Mail-Server

- **Serveradministrator.** Der Serveradministrator ist für das Warten, Installieren, Entfernen und Verwalten der Server im Netzwerk zuständig. Serveradministratoren sind zum Beispiel für folgende Aufgaben verantwortlich:
  - Verwalten der Software und der Daten, die sich auf den Netzwerkservern befinden
  - Verwalten der Hardware, die für die Netzwerkserver erforderlich ist
  - Installation und Konfiguration der angeforderten Betriebssysteme und Software
  - Entfernen von Servern
  - Protokollieren aller Aktionen/Statusänderungen im Anforderungsdatensatz
  - Bereitstellen des angeforderten Status
  - Empfehlungen für Verbesserungen hinsichtlich der Prozesse, Prozeduren und Tools
- **Prozessarchitekt.** Der Prozessarchitekt ist für die Serververwaltungsprozesse und -prozeduren zuständig. Prozessarchitekten sind für folgende Aufgaben verantwortlich:
  - Verwalten von Serververwaltungsprozeduren für eine Dienstbereitstellungsorganisation bzw. ein Konto
  - Entwickeln von Richtlinien für die Organisation/Konten
  - Informieren über neue/geänderte Richtlinien
  - Genehmigen/zurückweisen von Anforderungen, die von den Prozeduren abweichen
  - Unterstützen der Server-, Benutzer- und E-Mail-Administratoren bei der Implementierung der Prozesse/Prozeduren
  - Unterstützen bei der erneuten Zuordnung von fehlgeleiteten Anforderungen
  - Identifizieren einer möglichen Zuwiderhandlung gegen Dienststufenvereinbarungen für das Verarbeiten von Serververwaltungsanforderungen

- Kontakt zu Server-, Benutzer- und E-Mail-Administratoren aufnehmen zur Klärung möglicher Situationen, in denen Vereinbarungen nicht eingehalten werden
- Entwickeln und Erstellen von einem Paket für Dienststufenberichte für die Serververwaltung
- Entwicklung/Wartung von konten- und Tool-spezifischen Prozessen und Prozeduren aushandeln und organisieren
- den Prozessverantwortlichen Prozessvoraussetzungen und -erweiterungen darlegen
- Aktualisierungen für Betriebsprozesse überprüfen, genehmigen und implementieren

Sie sollten in Erwägung ziehen, die Zuständigkeiten zwischen leitenden und einfachen Administratoren aufzuteilen. Mit Tivoli SecureWay User Administration können Sie verschiedenen Mitarbeitern Berechtigungsklassen zuordnen.

Geschäftsanforderungen

Beim Erstellen des Einsatzes müssen nicht nur die Personen, denen Zugriffsberechtigungen für Benutzerkontoinformationen erteilt werden, sondern auch andere geschäftsumgebungsspezifische Punkte berücksichtigt werden. In der folgenden Liste sind einige dieser zu berücksichtigenden Punkte aufgeführt:

- **Datenvolatilität.** Wie oft werden Benutzerkonten hinzugefügt, geändert bzw. gelöscht?
- **Plattformheterogenität.** Auf welchen Plattformarten befinden sich die Benutzerkontoinformationen, die mit Tivoli SecureWay User Administration verwaltet werden sollen?
- **Anmeldeverfahren.** Werden sich die Benutzer an allen Plattformen und Maschinen auf dieselbe Weise anmelden? Oder sind für verschiedene Maschinen, Plattformen und andere Ressourcen unterschiedliche Anmeldeverfahren notwendig?
- **Benutzer-ID.** Können Benutzer eine allgemeine Benutzer-ID für verschiedene UNIX-Systeme verwenden?

- **Kennwort.** Können Benutzer ein allgemeines Kennwort für den Zugriff auf verschiedene Ressourcen verwenden oder ist für jede Ressource die Angabe eines eindeutigen Kennworts erforderlich? Welche Richtlinien gibt es hinsichtlich der Kennwortattribute, der Gültigkeitsdauer usw.?
- **Tools und Dienste.** Welche Tools und Dienste sind in der Umgebung vorhanden, die Benutzerkontoinformationen verwalten bzw. mit Tivoli SecureWay User Administration kommunizieren? Verwenden Sie beispielsweise NIS (NIS = Network Information System) zur Verwaltung von Benutzerkonten auf UNIX-Systemen? Verwenden Sie RACF (RACF = Resource Access Control Facility), das von OS/390 zur Verfügung gestellt wird? Wird Tivoli SecureWay User Administration zusammen mit anderen Tivoli-Produkten wie beispielsweise Tivoli SecureWay Security Manager eingesetzt?
- **Grafische Benutzerschnittstelle (GUI) oder Befehlszeile.** Werden die Mitarbeiter, die Tivoli SecureWay User Administration verwenden, hauptsächlich über die Befehlszeile oder die grafische Benutzerschnittstelle (GUI) arbeiten?
- **Vorhandene Verfahren ändern.** Falls einige dieser Verfahren (beispielsweise allgemeine Anmeldungen oder die Gültigkeitsdauer von Kennwörtern) nicht implementiert sind, sollen diese von Tivoli SecureWay User Administration implementiert werden? Sollen Verfahren implementiert werden, die zu Änderungen von Standardwertegruppen und Richtlinien für Gültigkeitsprüfung führen bzw. die die Verwendung von Tivoli Application Extension Facility erforderlich machen?
- **Produktanpassung.** Benötigen Sie für Ihre Umgebungen Erweiterungen, die nicht im Basisprodukt für Tivoli SecureWay User Administration enthalten sind? Werden Sie beispielsweise Tivoli Application Extension Facility verwenden, um benutzerdefinierte Funktionen zu erstellen?

Test

Es wird dringend empfohlen, dass Sie Tivoli SecureWay User Administration vor dem tatsächlichen Einsatz zunächst in einer Testumgebung implementieren. Sie sollten beim Erstellen Ihrer Testumgebung darauf achten, dass diese Ihrer Arbeitsumgebung so ähnlich wie möglich ist. Für das Erstellen der Testumgebung wird Folgendes empfohlen:

- Planen und Dokumentieren Sie die Testverfahren sorgfältig.
- Testen Sie alle Programmkorrekturen und Aktualisierungen.
- Testen Sie Teile des Einsatzentwurfs.
- Testen Sie die Erweiterungen für Tivoli SecureWay User Administration. Wenn Sie beispielsweise eine der folgenden Erweiterungen einsetzen möchten, sollten diese in Ihrer Testumgebung enthalten sein:
  - OS/390
  - AS/400
  - NIS
  - LDAP

  Anmerkung: Das Basisprodukt für Tivoli SecureWay User Administration umfasst Funktionen zur Verwaltung von Benutzerkonten auf UNIX-, Windows NT-, NetWare- und Windows 2000-Plattformen.
- Verwenden Sie dieselbe Softwareversion wie in Ihrer Arbeitsumgebung. Verwenden Sie beispielsweise dieselbe Version von Tivoli Management Framework, OS/390, NIS usw. wie in Ihrer Arbeitsumgebung.
- Führen Sie die Tests auf Maschinen aus, die bereits zu Arbeitszwecken eingesetzt wurden und auf denen bereits mehrfach verschiedene Softwareprodukte installiert wurden. (Führen Sie keine Tests auf ganz neuen Maschinen aus.)

4

Kennwortverwaltung

Es gibt drei Möglichkeiten, Kennwörter zu ändern, die in einem Benutzerprofil gespeichert sind: über den Befehl **wsetusr**, den Befehl **wpasswd** ohne die Optionen **–l** und **–L** und über die grafische Benutzerschnittstelle (GUI) zum Bearbeiten eines Benutzerdatensatzes. Die geänderten Kennwörter in einem Benutzerprofil können dann an die subskribierenden Endpunkte und verwalteten Knoten verteilt werden. Dabei können die Betriebssystemkennwörter des Endpunktes entweder mit dem Befehl **wdistrib** oder über die grafische Benutzerschnittstelle für Benutzerprofilverteilungen geändert werden. Mit dem Befehl **wpasswd** und der Option **–l** bzw. **–L** können durch die Ausgabe eines einzigen Befehls Kennwörter in Benutzerprofilen geändert und zugleich an die subskribierenden Endpunkte und verwalteten Knoten verteilt werden.

Die Änderungsfunktionen der GUI, die Befehle **wsetusr** und **wdistrib** sowie die Funktionen des Befehls **wpasswd**, die nur Systemadministratoren vorbehalten sind, sind nur für Tivoli-Administratoren auf verwalteten Knoten innerhalb der TMR verfügbar. Das für den Endbenutzer bestimmte Leistungsspektrum des Befehls **wpasswd** ist für alle Benutzer auf verwalteten Knoten und TMA-Endpunkten verfügbar.

Anmerkung: Die Kennwortverwaltungsfunktionen, die in Tivoli SecureWay User Administration integriert sind, sind nicht dazu gedacht, die Kennwort-Tools der verschiedenen verwalteten Betriebssysteme vollständig zu

ersetzen. Administratoren sollten die Entscheidung für ein bestimmtes Tool von den jeweiligen Gegebenheiten abhängig machen.

Befehl 'wpasswd' verwenden

Das Besondere an dem Befehl **wpasswd** ist, dass er nicht nur von Tivoli-Administratoren, sondern auch von anderen Benutzern ausgeführt werden kann. Mit diesem Befehl können allgemeine Kennwörter sowie die Kennwörter für bestimmte Konten (z. B. ein Windows NT-Kennwort) geändert werden. Darüber hinaus gibt es für den Befehl **wpasswd** verschiedene Optionen, über die festgelegt werden kann, wann und wo die Änderungen wirksam werden:

- Mit der Option **-L** wird das Kennwort auf allen Systemen geändert, die dem Benutzerdatensatz des betreffenden Benutzers zugeordnet sind.
- Mit der Option **-l** wird nur das Kennwort auf dem lokalen System geändert.
- Wird keine dieser Optionen angegeben, werden Änderungen des Kennworts erst bei der Verteilung des Benutzerprofils wirksam.

Der Befehl **wpasswd** steht für Benutzer nur zur Verfügung, wenn er auf Endpunkten unter Verwendung des Befehls **winstpw** installiert wurde. Eine Installation des Befehls **wpasswd** über die Arbeitsoberfläche oder SIS ist nicht möglich. Mit dem Befehl **winstpw** wird der Befehl **wpasswd** im Verzeichnis **$LCF_DATDIR/cache/bin/$INTERP/TME/WPASSGATEWAY** auf dem Endpunkt installiert. Anschließend sollte der Befehl **wpasswd** entweder in ein geeignetes Verzeichnis auf dem Endpunkt verschoben oder das Verzeichnis **$LCF_DATDIR/cache/bin/$INTERP/TME/WPASSGATEWAY** an den Benutzerpfad angehängt werden. Weitere Informationen zur Verzeichnisstruktur auf Endpunkten finden Sie im *Tivoli Management Framework Benutzerhandbuch*.

In der folgenden Tabelle sind die möglichen Verfahren zur Änderung von Benutzerkennwörtern sowie Hinweise zur Verwaltung von Kennwortänderungen aufgeführt.

Befehle bzw. Verfahren	Wird das neue Kennwort im Benutzerprofil gespeichert?	Wird das neue Kennwort auf den Subskriptions-zielen gespeichert?	Ist eine sofortige Benutzeranmeldung möglich?	Wird das Kennwort erst bei einer Verteilung des Benutzerprofils aktiviert?
wpasswd -L	Ja	Ja	Ja	Nein
wpasswd -l	Ja	Nein. Die Änderung wird auf dem Endpunkt gespeichert, auf dem der Befehl ausgeführt wurde, jedoch nicht an die anderen Subskribenten weitergegeben.	Ja, jedoch nur auf dem Endpunkt, auf dem der Befehl ausgeführt wurde.	Ja
wpasswd ohne **-L** oder **-l**	Ja	Nein	Nein	Ja
wcrtusr oder **wsetusr**	Ja	Nein	Nein	Ja
Betriebssystem-Tools für Kennwörter	Nein	Nicht zutreffend	Ja	Nein

Unter UNIX werden verschlüsselte Kennwörter verwendet. Bei der Datenweitergabe an Benutzerprofile von UNIX-Systemen aus werden UNIX-verschlüsselte Kennwörter zurückgegeben. Wenn ein Benutzer den Befehl **wpasswd** ausführt, um sein Kennwort für mindestens ein Benutzerprofil zu ändern, vergleicht Tivoli SecureWay User Administration das vom Benutzer angegebene Kennwort mit dem in den einzelnen Profilen vorhandenen Kennwort. Wenn die Datenweitergabe an das Konto von einem UNIX-System erfolgte und das UNIX-Kennwort nicht von einem Tivoli-Administrator geändert wurde, ist das vorhandene Kennwort noch nach UNIX-Standard verschlüsselt.

- Wird als TMR-Server ein UNIX-System eingesetzt, vergleicht das System mit Hilfe der von UNIX bereitgestellten Anwendungsprogrammierschnittstelle (API) **crypt**() das vom Benutzer angegebene Kennwort mit dem nach UNIX-Standard verschlüsselten Kennwort.
- Läuft der TMR-Server nicht unter UNIX, sondern zum Beispiel unter Windows NT, ist kein Vergleich mit nach UNIX-Standard verschlüsselten Kennwörtern möglich, da das Verschlüsselungsprogramm nicht verfügbar ist.

Bevor ein Endbenutzer sein UNIX-Kennwort auf einem TMR-Server ändern kann, der kein UNIX-System ist, aber von einem UNIX-Endpunkt seine Daten erhält, muss ein Tivoli-Administrator das UNIX-Kennwort festlegen.

Berechtigungsklassen für Kennwortänderungen

Für den Aufruf der administratorspezifischen Version des Befehls **wpasswd** benötigten Tivoli-Administratoren bisher die TMR-Berechtigungsklasse **admin**. Mit dieser Berechtigungsklasse erhielt der Administrator die Möglichkeit, alle Benutzerprofile, die den angegebenen Anmeldenamen enthalten, sowie alle Subskribenten dieser Benutzerprofildatensätze zu aktualisieren. Die administratorspezifische Version des Befehls **wpasswd** kann daher auch für die Synchronisation von Kennwörtern verwendet werden, während gleichzeitig verhindert wird, dass Kunden Administratorzugriffe im Zusammenhang mit Kennwortänderungen beeinflussen oder einschränken.

Die Berechtigungsklasse **Admin_Mod_Password** ermöglicht die Ausführung der administratorspezifischen Version des Befehls **wpasswd**, gestattet darüber hinaus jedoch keine Aktionen, für die in der Regel die Berechtigungsklasse **admin** erforderlich ist. Inwieweit der vom Administrator abgesetzte Befehl **wpasswd** ausgeführt wird, hängt davon ab, auf welche Benutzerprofile mit dem angegebenen Anmeldenamen der Administrator Zugriff hat. Beispiel:

- Verfügt der Administrator über die Berechtigungsklasse **admin** oder **Admin_Mod_Password**, werden die Änderungen an den Benutzerprofilen erfolgreich vorgenommen.
- Bei Anforderung einer sofortigen Weitergabe durch Angabe der Argumente **-l** oder **-L** bei Befehl **wpasswd** gilt dasselbe auch für die Subskribenten der Benutzerprofildatensätze.
  Mit der Berechtigungsklasse **Admin_Mod_Password** kann der Administrator keine Kennwörter über den Befehl **wsetusr** oder den Dialog **Benutzerprofilmerkmale** der Tivoli-Arbeitsoberfläche ändern. Um dem Administrator dies zu ermöglichen, muss ihm die Berechtigungsklasse **Admin_Edit_Account** oder **Admin_Mod_Account** zugeordnet werden; oder es müssen ihm eine bzw. mehrere Berechtigungsklassen zugeordnet werden, die Änderungen an Endpunktattributen ermöglichen.

Kennwörter und Endpunktarten

Tivoli SecureWay User Administration hat das Konzept der Endpunktart eingeführt (*eptype*), um die Objektklassen, die von Tivoli SecureWay User Administration verwaltet werden, zu abstrahieren. Jede Endpunktart entspricht einem Betriebssystem (UNIX, NT) bzw. einer Anwendung (LDAP, Policy Director), dessen bzw. deren Benutzer mit Hilfe von Tivoli SecureWay User Administration verwaltet werden.

Alle Endpunktarten werden Tivoli SecureWay User Administration durch Aufruf des Befehls 'waddusreptype' bekannt gegeben. Die Syntax dieses Befehls zeigt, dass alle Endpunktarten über unterschiedliche Merkmale verfügen:

```
waddusreptype –e
Endpunktartcode
–n Endpunktartname [–p
Attributpräfix] \
[–l Anmeldeattributname][–w Kennwortattributname] \
[–x Attributname für vorzeitigen Ablauf] [–xe Wert für Aktivierung des
vorzeitigen Ablaufs] \ [–xd Wert für
Inaktivierung des vorzeitigen Ablaufs] [–wl
maximale Kennwortlänge] \
[–cn Klassenname]
[–c Kontextattributname]
```

Für die Definition einer neuen Endpunktart gelten die folgenden Regeln:

- Jeder Endpunktart ist ein langer *Endpunktname*, der angezeigt wird, und ein kurzer *Endpunktcode* zur Eingabe zugeordnet.
- Alle Endpunktartattributnamen müssen mit einem eindeutigen *Attributpräfix* beginnen.
- Es muss ein Anmeldeattribut angegeben werden.
- Es muss ein Kennwortattribut angegeben werden.
- Wenn der vorzeitige Kennwortablauf unterstützt wird, müssen der Name des Attributs für den vorzeitigen Kennwortablauf sowie gültige Werte für dieses Attribut angegeben werden, die anzeigen, ob der vorzeitige Kennwortablauf aktiviert oder inaktiviert werden soll.
- Wenn die Länge des Kennworts begrenzt ist, muss diese Länge angegeben werden.
- Wenn die Anmeldung durch einen Kontext (wie beispielsweise NetWare und Windows 2000) qualifiziert ist, muss das Attribut mit dem Kontext angegeben werden.
- Wenn es sich bei der Endpunktart um eine Anwendung handelt, muss der Klassenname der Objektimplementierung angegeben werden.

Anmerkungen:

1. Die meisten Informationen, die für den Befehl **waddusreptype** angegeben werden, unterstützen die Kennwortänderung auf Endpunkten mit dem Befehl **wpasswd** .
2. Ein Benutzerdatensatz enthält Informationen zu einer bestimmten Endpunktart, wenn diesem Benutzerdatensatz ein Wert für das Anmeldeattribut der Endpunktart zugeordnet ist. Aus diesem Grund ignoriert Tivoli SecureWay User Administration die Angabe bzw. Änderung von Attributen, einschließlich des Kennworts, für Endpunktarten, für die dem Benutzer keine Anmeldeberechtigungen erteilt wurden.

3. Wenn Sie den Befehl **wpasswd –et** bzw. **wlsusreptype** absetzen, wird eine Liste mit allen Endpunktartnamen und -codes, die von einer TMR unterstützt werden, angezeigt.

Allgemeine und endpunktartspezifische Kennwörter

In jedem Benutzerdatensatz können zwei Arten von Kennwörtern enthalten sein: das *allgemeine* Kennwort und das *endpunktartspezifische* Kennwort. Über das allgemeine Kennwort können alle Kennwörter im Benutzerdatensatz geändert werden. Das allgemeine Kennwort hat jedoch keinen direkten Einfluss auf die Kennwörter, die vom Benutzer eingegeben werden, wenn er sich an einem System bzw. einer Anwendung anmeldet, die von Tivoli SecureWay User Administration verwaltet werden. Endpunktartspezifische Kennwörter haben diese Funktion.

Die anderen Kennwörter in einem Benutzerdatensatz sind *endpunktartspezifische* Kennwörter. Bei integrierten Endpunktarten (UNIX, NT und NetWare) verfügen die Befehle **wcrtusr/wsetusr/wgetusr** über bestimmte Optionen für das Setzen und Abrufen von Kennwortattributen:

-p UNIX-Kennwort
-pt NT-Kennwort
-pw NetWare-Kennwort

Bei anderen Endpunktarten, die Tivoli SecureWay User Administration unter Verwendung von AEF hinzugefügt wurden, müssen Sie den Namen des zu bearbeitenden Kennwortattributs kennen.

Für diese Endpunktarten verwenden die Befehle **wcrtusr/wsetusr/wgetusr** die generische Option **–x** *Attributname* für das Setzen und Abrufen der Kennwörter.

Für die im Lieferumfang von Tivoli SecureWay User Administration Version 3.8 enthaltenen Endpunktarten lauten diese Endpunktartnamen und die zugehörigen Kennwortattribute wie folgt:

Endpunktartname	Kennwortattributname
LDAP	sso_password
OS/2	os2_password
OS400	OS400_PassW
Policy Director	PD_Password
RACF	racf_password
Windows 2000	w2k_password

Nur das allgemeine Kennwort ändern

Normalerweise werden Änderungen des allgemeinen Kennworts an alle Kennwörter in diesem Datensatz weitergegeben. Es gibt jedoch zwei Möglichkeiten, um nur das allgemeine Kennwort zu ändern und die Weitergabe zu unterdrücken. Zum einen können Sie das LDAP-Kennwort, das das Attribut des allgemeinen Kennworts **sso_password** als endpunktartspezifisches Kennwortattribut verwendet, ändern:

```
wpasswd –c LDAP Benutzer1
```

Zum anderen können Sie die vorhandenen Kennwörter für die definierten Endpunktartkennwörter angeben. Dadurch wird nur das allgemeine Kennwort geändert:

```
wpasswd –cp allg-KW –p vorh-UNIX-KW @UserProfile:up1 Benutzer1
```

Im oben angegebenen Beispiel entspricht das angegebene UNIX-Kennwort dem vorhandenen Kennwort, so dass das Hot Flag und die Versionsnummer für das UNIX-Kennwort nicht gesetzt bzw. geändert werden.

Kennwortänderung durch Benutzer steuern

Einigen Endpunktarten (NetWare, NT, OS/2 und UNIX) ist ein Attribut zugeordnet, über das ein Administrator steuern kann, ob ein Endbenutzer dazu berechtigt ist, Benutzerkennwörter zu ändern. Diese Attribute werden bei der Verteilung von Benutzerprofilen berücksichtigt: wenn ein Endbenutzer nicht dazu berechtigt ist, ein Kennwort zu ändern, wird das Endpunktkennwort jedes Mal von einem verteilten Kennwort überschrieben, wenn eine Push-Operation für den Benutzerdatensatz ausgeführt wird. Einige Plattformen (AIX, OS/2) stellen eine systemeigene Unterstützung für die allein Administratoren vorbehaltene Kennwortsteuerung zur Verfügung.

Endpunktart	Option	wsetusr-Werte	GUI-Anzeige	GUI-Eingabeaufforderung
NetWare	-cw	AKTIVIERT/ INAKTIVIERT	NetWare-Kennwort	Änderung durch Benutzer zulassen
Windows NT	-ct	AKTIVIERT/ INAKTIVIERT	NT-Kennwort	Änderung durch Benutzer zulassen
UNIX	-o	AKTIVIERT/ INAKTIVIERT	UNIX-Kennwort	Benutzersteuerung Administratorssteuerung

Von den Endpunktarten, die Tivoli SecureWay User Administration unter Verwendung von AEF hinzugefügt wurden, unterstützen nur OS/2 und Windows 2000 die alleinige Kennwortsteuerung durch den Administrator:

Endpunktart	Option	wsetusr-Werte	GUI-Anzeige	GUI-Eingabeaufforderung
OS/2	-x os2_password_\ admin_only	Ja | Nein	OS/2-Konto	Änderung durch Benutzer zulassen
Windows 2000	-x w2k_uf_\ password_\ cant_change	AKTIVIERT/ INAKTIVIERT	Windows 2000-Kennwort	Änderung durch Benutzer nicht zulassen

Kennwortqualitätsregeln

Die Kennwortqualitätsregeln, die von Tivoli SecureWay Security Manager sowohl für globale als auch endpunktartspezifische Systemrichtlinien unterstützt werden, können über die Befehle **wpasswd** und **wsetusr** auf dem Server angewendet werden. Die Durchsetzung der Qualitätsregeln wird für einen bestimmten Benutzerdatensatz aktiviert, indem eine Verbindung zwischen diesem Datensatz und einem Systemrichtliniendatensatz in einem Sicherheitsprofil hergestellt wird. Diese Verbindung wird mit der Option **–sp** der Befehle **wcrtusr/wsetusr** hergestellt. Diese Option wird wie folgt verwendet:

```
-sp <secpol-name>:<syspolrec-name>
```

wobei <secpol-name> der Name des Sicherheitsprofils, der den gewünschten Systemrichtliniendatensatz enthält (mit oder ohne die Initiale @SecurityProfile:), und <syspolrec-name> der Name des gewünschten Systemrichtliniendatensatzes ist.

Für das Attribut syspolrec können Standardwertegruppen verwendet werden, um alle Benutzerdatensätze in einem Benutzerprofil mit demselben Systemrichtliniendatensatz zu verbinden. Gesetzt den Fall, ein Systemrichtliniendatensatz mit dem Namen “Qualitätsregeln” befindet sich im Sicherheitsprofil “sp1”. Dann würde mit dem folgenden CLI-Befehl die Standardwertegruppe erstellt, die allen im Benutzerprofil “up1” erstellten Benutzern diesen Systemrichtliniendatensatz zuordnet:

```
wputpolm –d –c "1825034724.1.762#SECURITYP::SecurityProfile#\
;Qualitätsregeln" @UserProfile:up1 syspolrec
```

Anmerkung: Im Befehl **wputpolm** wird die **Objekt-ID (OID)** und nicht der Name des Sicherheitsprofils verwendet. Die **Objekt-ID (OID)** und der Name des Systemrichtliniendatensatzes werden durch ein Semikolon voneinander getrennt und nicht durch einen Doppelpunkt wie in der Option **wsetusr –sp**.

Wenn diese Verbindung hergestellt wurde, werden alle späteren Kennwortänderungen im Benutzerdatensatz anhand der Kennwortrichtlinien des Systemrichtliniendatensatzes überprüft. Es werden keine Kennwortänderungen vorgenommen, wenn ein neues Kennwort den festgelegten Qualitätsregeln nicht entspricht. Die globale Kennwortrichtlinie von Tivoli SecureWay User Administration wird stets auf Änderungen des allgemeinen Kennworts angewendet. Eine endpunktartspezifische Kennwortrichtlinie wird nur dann angewendet, wenn ein Kennwort für diese Endpunktart geändert wird. Ob globale Systemrichtlinien angewendet werden können, wenn nur das Kennwort einer bestimmten Endpunktart geändert wird, hängt von den Einstellungen im Kennwortrichtliniendatensatz ab.

Der CLI-Befehl in Tivoli SecureWay Security Manager zum Festlegen der Werte für die Attribute des Systemrichtliniendatensatzes in Tivoli SecureWay User Administration (ausführliche Informationen hierzu finden Sie im Handbuch *Tivoli SecureWay User Administration Reference Manual*) lautet:

wmodsec Systemrichtlinie [**-s** *Attribut=Wert*]... *Profil Datensatzname*

wobei das Attribut folgendes Format hat: [<Endpunktartcode>] <Attributname>. Wenn der <Endpunktartcode> weggelassen wird, ist das Attribut ein globales Systemrichtlinienattribut und wird auf das allgemeine Kennwort (und somit auf alle Kennwörter) angewendet, wenn das allgemeine Kennwort mit dem Befehl **wpasswd** geändert wird. Wenn für den <Endpunktartcode> eine Angabe gemacht wird, wird dieser Attributwert nur auf Kennwörter für diese Endpunktart angewendet. Beispiel: **UXPwMaxReps** gibt die maximale Anzahl an Zeichen an, die in einem UNIX-Kennwort wiederholt angegeben werden dürfen, **PwMaxReps** gibt die globale maximale Anzahl an Zeichen an, die in Kennwörtern wiederholt angegeben werden dürfen. Wenn das allgemeine Kennwort geändert wird, wird der Wert **PwMaxReps** auf alle Kennwörter einschließlich der NT- und RACF-Kennwörter, die über kein entsprechendes endpunktartspezifisches Attribut verfügen, angewendet.

Anmerkung: Für diesen Befehl gibt es noch weitere Optionen, die hier nicht beschrieben werden. Weitere Informationen finden Sie in der Beschreibung des Befehls **wmodsec** im *Tivoli SecureWay Security Manager Benutzerhandbuch*.

Unterstützte Security Manager-Kennwortrichtlinien

Im Folgenden werden die für Systemrichtliniendatensätze in Tivoli SecureWay Security Manager geltenden Kennwortrichtlinienattribute aufgelistet, die von den Befehlen **wpasswd** und **wsetusr** umgesetzt werden:

PwChk , UXPwChk

Gibt an, ob die Kennwortüberprüfung auf Subskriptionsendpunkten aktiviert ist und ob diese Qualitätsregeln vom Admin-Server angewendet werden. Gültige Werte sind 'True' und 'False'.

PwContUid

Gibt an, ob die GSO-Benutzer-ID im Kennwort enthalten sein darf. Gültige Werte sind **True** und **False**.

PwHistory, NTPwHistory, UXPwHistory, OS2PwHistory, OS4PwHistory, RFPwHistory

Gibt an, wie viele bisherige Kennwörter gespeichert werden sollen, um die Wiederverwendung alter Kennwörter zu verhindern. Gültige Werte sind **None** oder jede ganze Zahl, die größer ist als Null. Tivoli SecureWay User Administration ruft den jeweils maximalen Wert ab und verwaltet einen Protokoll-Stack mit dieser Tiefe, die für Überprüfungen verwendet wird und die unabhängig davon, welches Kennwort geändert wird, aktualisiert wird. Die tatsächliche Tiefe, die nach Änderungen an einem Kennwort einer bestimmten Endpunktart überprüft wird, wird durch den Attributwert xxPwHistory für diese Endpunktart gesteuert.

PwMaxLen

Gibt die Anzahl an Zeichen an, die ein Kennwort maximal enthalten darf. Gültige Werte sind 0 bis 65535. Der Standardwert ist 8. Da es sich hierbei um eine globale Richtlinie handelt, sollten Sie diese nicht mit Tivoli SecureWay User Administration verwenden. Eine einzige globale Attributeinstellung ist nicht für alle Endpunktarten geeignet, dennoch wird Tivoli SecureWay User Administration sie auf alle Endpunktarten anwenden, wenn das allgemeine Kennwort geändert wird.

PwMaxReps, UXPwMaxReps, OS4PwMaxReps

Gibt die maximale Anzahl von sich wiederholenden Zeichen an, die das Kennwort enthalten darf. Der Wert dieses Attributs muss eine ganze Zahl sein, die größer als oder gleich Null ist.

PwMinAge, NTPwMinAge, UXPwMinAge, OS2PwMinAge

Gibt die Mindestanzahl an Tagen an, die vergehen müssen, bevor der Benutzer das Kennwort ändern kann. Gültige Werte sind **Now**, d. h. der Benutzer kann das Kennwort jederzeit ändern, oder jede ganze Zahl, die größer als Null ist.

PwMinAlphanums, UXPwMinAlphanums

Gibt die Mindestanzahl an alphanumerischen Zeichen (a-z, A-Z, 0-9) an, die im Kennwort vorkommen müssen. Der Wert dieses Attributs muss eine ganze Zahl sein, die größer als oder gleich Null ist.

PwMinAlphas, UXPwMinAlphas

Gibt die Mindestanzahl an alphabetischen Zeichen (a-z, A-Z) an, die im Kennwort vorkommen müssen. Der Wert dieses Attributs muss eine ganze Zahl sein, die größer als oder gleich Null ist.

PwMinDiff

Gibt die Mindestanzahl an Zeichen im neuen Kennwort an, die sich von den Zeichen des alten Kennworts unterscheiden müssen. Gültige Werte sind 0 bis 65535. Der Standardwert ist 2. Beachten Sie, dass die Durchsetzung dieser Qualitätsregel mit dem Befehl wpasswd nicht immer möglich ist. Wenn der Benutzerdatensatz von einem Endpunkt aus weitergegeben wurde, ist das alte Kennwort möglicherweise nicht verfügbar bzw. UNIX-verschlüsselt.

PwMinLen, NTPwMinLen, UXPwMinLen, OS4PwMinLen, OS2PwMinLen

Gibt die Mindestanzahl an Zeichen an, die im Kennwort vorkommen müssen. Der Wert dieses Attributs muss eine ganze Zahl sein, die größer als oder gleich Null ist. Der Wert Null gibt an, dass Kennwörter beliebig lang sein dürfen und die Kennwortlänge nicht überprüft wird.

PwMinLowers, UXPwMinLowers

Gibt die Mindestanzahl an alphabetischen Zeichen in Kleinschreibung (a-z) an, die im Kennwort vorkommen müssen. Der Wert dieses Attributs muss eine ganze Zahl sein, die größer als oder gleich Null ist.

PwMinNums, UXPwMinNums

Gibt die Mindestanzahl an Zahlen (0-9) an, die in einem Kennwort enthalten sein müssen. Der Wert dieses Attributs muss eine ganze Zahl sein, die größer als oder gleich Null ist.

PwMinOther

Gibt die Mindestanzahl an anderen, nichtalphabetischen Zeichen an, die in einem Kennwort enthalten sein müssen. Gültige Werte sind 0 bis 65535. Der Standardwert ist 0.

PwMinSpecials, UXPwMinSpecials

Gibt die Mindestanzahl an Sonderzeichen an, die im Kennwort vorkommen müssen. Ein Sonderzeichen ist jedes nicht alphanumerische Zeichen. Der Wert dieses Attributs muss eine ganze Zahl sein, die größer als oder gleich Null ist.

PwMinUppers, UXPwMinUppers

Gibt die Mindestanzahl an alphabetischen Zeichen in Großschreibung (A-Z) an, die im Kennwort vorkommen müssen. Der Wert dieses Attributs muss eine ganze Zahl sein, die größer als oder gleich Null ist.

Damit die RACF-Qualitätsregeln für Kennwörter, **RFPwRules** und **RFPwSyntax**, angewendet werden können, muss das neue Kennwort in die IBM US-Codepage übersetzt werden. Darüber hinaus muss Tivoli SecureWay User Administration alle alphabetischen Zeichen in Großbuchstaben umsetzen.

RFPwRules

Sie können bis zu acht Regeln für RACF-Kennwörter angeben (durch Kommas voneinander getrennt). Kennwörter, die mindestens eine der definierten Regeln erfüllen, werden von RACF akzeptiert. Jede Regel besteht aus den folgenden drei Komponenten, die durch Doppelpunkte voneinander getrennt sind:

- eine Mindestlänge
- wahlweise eine maximale Länge
- eine Zeichenfolge, die angibt, welche Art von Zeichen innerhalb der definierten Längengrenzwerte verwendet werden dürfen.

Die einzelnen Regeln werden aktiviert, indem Sie als Mindestlänge eine andere Zahl als Null angeben. Alle vorhandenen Regeln können inaktiviert werden, indem Sie die Mindestlänge auf den Wert Null setzen. Wenn für die maximale Länge der Wert Null angegeben wird, gilt die Regel nur für Kennwörter mit der von Ihnen im Feld 'Minimale Länge' angegebenen Länge. Wenn Sie für die maximale Länge einen anderen Wert als Null eingeben möchten, muss dieser Wert größer als oder gleich dem Wert für die minimale Länge sein. Es spielt keine Rolle, in welcher Reihenfolge Sie die Regeln definieren. Über die angegebene Zeichenfolge können Sie definieren, welche Art von Zeichen in der jeweiligen Position innerhalb des vom Benutzer einge-

gebenen Kennworts gültig sein soll. In der folgenden Liste finden Sie eine Beschreibung der Codes, die in der Zeichenfolge verwendet werden können:

- A = Alphabetische Zeichen und die Sonderzeichen #, $, und @
- C = Konsonanten
- L = Alphanumerische Zeichen. Dazu gehören alphabetische Zeichen, numerische Zeichen und die Sonderzeichen #, $ und @. Wenn in der Kennwortregel “L” angegeben wird, muss das Kennwort mindestens ein alphabetisches Zeichen oder eines der Sonderzeichen sowie ein numerisches Zeichen enthalten.
- N = Numerische Zeichen
- V = Vokale ’A’, ’E’, ’I’, ’O’ und ’U’
- W = Konsonanten, Sonderzeichen und numerische Zeichen
- * = beliebiges alphanumerisches Zeichen

Im folgenden Beispiel wird eine Regel definiert, die angibt, dass ein Kennwort acht Zeichen mit Konsonanten in den Positionen 1, 3, 5, 6 und 8, sowie Zahlen in den Positionen 2 und 4 enthalten muss:

```
8:0:CNCNCC*C
```

RFPwSyntax

Wenn der Wert auf T (True) gesetzt ist, werden RACF-Kennwörter anhand der Kriterien, die für das Attribut RFPwRules angegeben wurden, überprüft. Der Standardwert lautet F (False).

Nicht unterstützte Security Manager-Kennwortrichtlinien

Im Folgenden werden die für die Tivoli SecureWay Security Manager-Systemrichtliniendatensätze geltenden Kennwortrichtlinienattribute aufgelistet, deren Richtlinien von den Befehlen **wpasswd** und **wsetusr** nicht umgesetzt werden:

PwDictFile

Eine Dateispezifikationszeichenfolge, die den Pfadnamen einer GSO-Kennwortdatei mit Einträgen (ein Eintrag pro Zeile) ungültiger Kennwörter angibt. Gültige Werte sind **None** oder ein Pfadname für eine Datei. Der Standardwert ist **None**. Da die Angabe dieses Pfadnamens von den Einstellungen für die Umgebungsvariablen auf dem GSO-Server abhängig ist, ist eine zuverlässige Lokalisierung dieser Datei auf dem TMR-Server durch Tivoli SecureWay User Administration nicht möglich.

PwMaxAge, NTPwMaxAge, UXPwMaxAge, OS2PwMaxAge, OS4PwMaxAge, RFPwMaxAge

Gibt die maximale Anzahl von Tagen an, die vergehen dürfen, bevor der Benutzer das Kennwort ändern muss. Gültige Werte sind **Unlimited** oder jede ganze Zahl, die größer als Null ist. Nur Endpunkte können feststellen, ob die maximale Gültigkeitsdauer (**MaxAge**) eines Kennworts überschritten wurde, so dass die Umsetzung dieser Richtlinie durch Tivoli SecureWay User Administration auf dem Server nicht möglich ist.

Windows 2000-Kennwortrichtlinien

Die vorherigen Abschnitte enthalten keine Informationen zu Windows 2000-Kennwortrichtlinien. Der Grund hierfür ist, dass Tivoli SecureWay Security Manager zum Zeitpunkt der Veröffentlichung dieses Handbuchs keine Windows 2000-Systemrichtlinien unterstützte. Wenn Tivoli SecureWay Security Manager eine Unterstützung für Windows 2000-Systemrichtlinien zur Verfügung stellt, wird Tivoli SecureWay User Administration Version 3.8 alle Windows 2000-Kennwortrichtlinien mit Attributnamen, die den oben angezeigten Namen ähnlich sind, automatisch umsetzen. Wenn das Kennwortrichtlinienattribut **W2KPwHistory** von Tivoli SecureWay Security Manager unterstützt wird, wird Tivoli SecureWay User Administration Version 3.8 die zugehörige Richtlinie umsetzen, da es alle Attribute im Format **<Endpunktartcode>PwHistory** umsetzt.

Durchsetzung durch den Server oder Durchsetzung durch den Endpunkt

Tivoli SecureWay Security Manager kann die in den Sicherheitsprofilen definierten Systemrichtlinien an die Endpunkte verteilen. Diese Systemrichtlinien enthalten Kennwortrichtlinien, die immer dann angewendet werden, wenn ein Kennwort durch die Sicherheitskomponente des jeweiligen Endpunkts (z. B. durch RACF unter OS/390, Tivoli Access Control Facility (Tivoli ACF) unter UNIX, Benutzer-Manager unter NT) geändert wird. Wenn Tivoli SecureWay User Administration ein neues Kennwort an die Endpunkte verteilt, an die Tivoli SecureWay Security Manager eine Kennwortrichtlinie verteilt hat, wird von den jeweiligen Endpunkten eine Fehlermeldung generiert, wenn das neue Kennwort nicht der Kennwortrichtlinie entspricht.

Da Tivoli SecureWay User Administration die Durchsetzung der Kennwortrichtlinien durch den Server unterstützt, kann diese Vielzahl von Endpunktnachrichten durch eine einzige Servernachricht ersetzt werden. Dazu sollte die für einen Benutzer auf dem Server geltende Systemrichtlinie mindestens so strikt sein wie die Systemrichtlinie, die an die Endpunkte verteilt wurde. Idealerweise sollte die für einen Benutzer geltende Systemrichtlinie auf dem Server mit der verteilten Systemrichtlinie *identisch* sein.

Wenn sie nicht synchronisiert werden können, werden neue Kennwörter möglicherweise weiterhin von einigen Endpunkten zurückgewiesen.

Meldung von Verstößen gegen Kennwortrichtlinien

Administratoren betrachten möglicherweise die Anzeige der Kennwortrichtlinien, die ein Kennwort nicht erfüllt, als Sicherheitsrisiko. Aus diesem Grund ist es möglich, diese Funktion mit dem Befehl **wsetusrcfg** zu inaktivieren. Wenn die Anzeige von Verstößen gegen die Kennwortrichtlinie aktiviert ist (Standardeinstellung), wird Folgendes angezeigt, wenn “aaa” als neues UNIX- und NT-Kennwort für einen Benutzer angegeben wird, dem die Standardkennwortrichtlinien von Tivoli SecureWay Security Manager zugeordnet wurden:

```
wpasswd -c UX -c NT user2
Neues Kennwort:
Neues Kennwort erneut eingeben:
Ihr neues Kennwort wurde zurückgewiesen.
Das Kennwort hat die NT-Qualitätsregeln  nicht erfüllt, da in den ersten
14 Zeichen folgender Fall aufgetreten ist:
    - enthält weniger als 5 Buchstaben.
Das Kennwort hat die UX-Qualitätsregeln  nicht erfüllt, da in den ersten
8 Zeichen folgender Fall aufgetreten ist:
    - enthält ein Zeichen, das mehr als 2 Male verwendet wird.
    - enthält weniger als 4 Buchstaben.
    - enthält weniger als 1 numerisches Zeichen.
    - enthält weniger als 1 Sonderzeichen.
    - enthält weniger als 1 Großbuchstaben.
```

Leistungsspektrum von wpasswd

Der Befehl **wpasswd** hat viele verschiedene Funktionen, da er sowohl über einen TMA-Endpunkt als auch über einen verwalteten Knoten ausgeführt werden kann. Alle diese Funktionen betreffen mehr oder weniger das Konzept der Kennwortverwaltung. Der Befehl **wpasswd** hat viele verschiedene Funktionen, die von den verwendeten Optionen abhängen. In den folgenden Abschnitten wird vorausgesetzt, dass der Leser mit der Basissyntax des Befehls **wpasswd** vertraut ist. Eine Beschreibung der Befehlssyntax finden Sie im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Kennwörter ändern

Die Grundfunktion des Befehls 'wpasswd' ist die Änderung von Kennwörtern in Benutzerprofilen. Der verwendete Anmeldename und die angegebenen Optionen sind ausschlaggebend dafür, welche Kennwörter in welchen Profilen geändert werden können.

Nur Benutzerprofilkennwörter aktualisieren

Bei Endbenutzern stellt sich nicht die Frage, unter welchem Kennwort gearbeitet wird. Es ist der Anmeldename, mit dem sich der Endbenutzer angemeldet hat. Administratoren können einen Anmeldenamen angeben oder den Anmeldenamen übergehen und unter ihrem eigenen Anmeldenamen arbeiten.

Nach Feststellung des Anmeldenamens lokalisiert der Befehl **wpasswd** alle Benutzerdatensätze in allen Benutzerprofilen in der TMR, die diesen Anmeldenamen enthalten. Jede Verwendung dieses Benutzernamens ist notwendigerweise einer bestimmten Endpunktart (oder dem allgemeinen Kennwort) zugeordnet. Wenn der Benutzer die Option **–c Endpunktartcode** im Befehl **wpasswd** verwendet, kann er die zu ändernden Endpunktartkennwörter auswählen. Wenn die Option **–c** nicht angegeben wird, wird das allgemeine Kennwort geändert. Entsprechend den Weitergaberichtlinien des allgemeinen Kennworts, werden durch die Änderung des allgemeinen Kennworts alle Kennwörter in einem Benutzerdatensatz geändert. Bei Verwendung des Befehls 'wpasswd' wird diese Regel etwas erweitert: wenn das allgemeine Kennwort geändert wird, werden alle Kennwörter in allen Datensätzen, die den angegebenen Anmeldenamen enthalten, geändert. Bei Verwendung einer oder mehrerer **–c Endpunktartcode**-Optionen werden nur die Kennwörter für die angegebene(n) Endpunktart(en) geändert.

-l => ...und lokalen Host aktualisieren

Wenn beim Aufruf des Befehls 'wpasswd' die Option **–l** verwendet wird, wird das Benutzerkennwort auf dem System, auf dem der Befehl 'wpasswd' ausgegeben wurde, geändert, nachdem die Benutzerkennwörter in den Benutzerprofilen geändert wurden. Sie können über die Optionen **–c Endpunktartcode** auch die Endpunkt-

arten begrenzen, auf denen Kennwortänderungen ausgeführt werden. Beispiel: Wenn ein Benutzer mit dem Namen “sandy” auf einem UNIX-System mit dem Namen “bear” den Befehl

```
wpasswd –c NT –l
```

ausgibt, werden alle NT-Kennwörter des Benutzers ’sandy’ in den Benutzerprofilen geändert, jedoch wird das Kennwort des Benutzers ’sandy’ auf dem System ’bear’ nicht geändert.

-L => ...und alle Subskribenten aktualisieren

Wenn beim Aufruf des Befehls **wpasswd** die Option **–L** verwendet wird, wird das Benutzerkennwort auf “allen subskribierenden Endpunkten” geändert, nachdem die Benutzerkennwörter in den Benutzerprofilen geändert wurden. Um festzustellen, welche Endpunkte dies sind, bestimmt der Befehl **wpasswd** zunächst alle Benutzerprofile, in denen Benutzerkennwörter geändert wurden. Daraufhin werden die Profilmanager identifiziert, zu denen diese Benutzerprofile gehören. Danach werden die Subskriptionsbaumstrukturen dieser Profilmanager erweitert und alle Endpunkte, die Zieladressen für Verteilungen dieser Profilmanager und Subskriptionen auf Datensatzebene sein könnten, identifiziert. Aus dieser Endpunktgruppe werden Endpunkte entfernt, so dass die Gruppe nur noch die Endpunkte der Endpunktarten, die über die Argumente **–c Endpunktartcode** angegeben wurden, enthält. Schließlich wird das Benutzerkennwort auf diesen Endpunkten zeitgleich unter Verwendung der Framework-Funktion **mdist** geändert.

Meldungen über erfolgreiche/fehlerhafte Operationen

Wenn keine ausführliche Anzeige angefordert wurde (d. h. wenn die Option **–v** nicht verwendet wurde), werden nur Nachrichten ausgegeben, wenn bei Änderungen von Endpunktkennwörtern Ausnahmen aufgetreten sind. Dies bedeutet, dass nur die Namen der Endpunkte angezeigt werden, für die eine Kennwortänderung nicht erfolgreich ausgeführt werden konnte und die eine Ausnahmebedingung zurückgegeben haben. Die Nachrichten, die von einem Endpunkt ausgegeben werden, werden immer angezeigt. Einige Endpunkte geben zwar Fehlermeldungen, jedoch keine Ausnahmebedingungen zurück. Der

Befehl **wpasswd** gibt leider keine Fehlermeldungen für diese Endpunkte aus, auch wenn die für diese Endpunkte ausgeführte Operation eindeutig fehlerhaft war. Halten Sie sich an die Nachrichten.

Nach erfolgreicher Ausführung des Befehls **wpasswd –L** wird normalerweise folgende Meldung ausgegeben:

```
wpasswd -L user2
Neues Kennwort:
Neues Kennwort erneut eingeben:
Die Administrator-Kennwortänderung für Benutzername user2 wurde
erfolgreich ausgeführt:
LDAP-/SSO-/UX-Kennwort für user2 in Benutzerprofil pm1.up1 geändert
LDAP-/NT-/NW-/SSO-/W2K-/OS4-/OS2-/RF-/UX-Kennwort für user2 in
Benutzerprofil pm1.up2 geändert
Alle Kennwortänderungen auf Endpunkten waren erfolgreich.
```

Im Verbose-Anzeigemodus werden Meldungen für alle erfolgreichen bzw. fehlerhaften Kennwortänderungen auf Endpunkten sowie Berichte über Ausnahmen, die oben beschrieben wurden, ausgegeben:

```
wpasswd -L -v user2
Neues Kennwort:
Neues Kennwort erneut eingeben:
Die Administrator-Kennwortänderung für Benutzername user2 wurde
erfolgreich ausgeführt:
LDAP-/SSO-/UX-Kennwort für user2 in Benutzerprofil pm1.up1 geändert
LDAP-/NT-/NW-/SSO-/W2K-/OS4-/OS2-/RF-/UX-Kennwort für user2 in
Benutzerprofil pm1.up2 geändert
Änderung des Kennworts wurde auf folgenden UX-Endpunkten erfolgreich
ausgeführt: bear, lgrenin2-ep.
Alle Kennwortänderungen auf Endpunkten waren erfolgreich.
```

Dienstprogrammfunktionen

Die folgenden Funktionen führen **wpasswd**-Dienstprogrammtasks aus:

-ul => nur NT-Konto freigeben

Endbenutzer bzw. Tivoli-Administratoren können NT-Konten mit dem Befehl **wpasswd –ul** freigeben. Dieser Befehl sendet an alle NT- und Windows 2000-Endpunkte, die Subskribenten des Benutzerdatensatzes sind, eine Freigabeanforderung.

-et => nur Endpunktartnamen und -codes anzeigen

Da sowohl Endbenutzer als auch Administratoren die Namen und Codes der Endpunktarten, die von der TMR unterstützt werden, kennen müssen, um die Option **–c** des Befehls 'wpasswd' verwenden zu können, kann durch Verwendung der Option **–et** des Befehls 'wpasswd' eine Liste mit den Namen und Codes der Endpunktarten aufgerufen werden. Da der Befehl **wlsusreptype** nur von Administratoren und nicht von Endbenutzern verwendet werden kann, wurde diese Funktion dem Befehl **wpasswd** zugeordnet. Standardmäßig zeigt Tivoli SecureWay User Administration folgende Endpunktarten an:

```
Namen und Codes der Endpunktarten:
        Common      SSO
        LDAP        LDAP
        NT          NT
        NetWare     NW
        OS/2        OS2
        OS400       OS4
     PolicyDirector PD
        RACF        RF
        UNIX        UX
        W2K         W2K
```

-qr => nur Qualitätsregeln für Benutzer anzeigen

Beim Erstellen eines neuen Kennworts möchten Endbenutzer wissen, welche Richtlinien für dieses neue Kennwort gelten. Mit dem Befehl **wpasswd –qr** können Sie eine Liste mit den für das Benutzerkennwort geltenden Richtlinien aufrufen. Administratoren betrachten die Anzeige von Kennwortrichtlinien möglicherweise als Sicherheitsrisiko. Aus diesem Grund ist es möglich, diese Funktion mit dem Befehl **wsetusrcfg** zu inaktivieren. Wenn der Benutzer mit dem Namen "user2", der einem Tivoli SecureWay Security Manager-Systemrichtliniendatensatz zugeordnet ist, für den die Standardwertegruppen gelten, lediglich die UNIX-Richtlinien anfordert, wird Folgendes angezeigt:

```
Benutzer user2 in Benutzerprofil pm1.up2 verwendet folgende Regeln...
Das Kennwort erfüllt die UX-Qualitätsregeln nicht, da in den ersten
8 Zeichen folgender Fall aufgetreten ist:
    - enthält ein Zeichen, das mehr als 2 Male verwendet wird.
    - enthält weniger als 1 alphanumerisches Zeichen.
    - enthält weniger als 4 Buchstaben.
```

```
- enthält weniger als 1 Kleinbuchstaben.
- enthält weniger als 1 numerisches Zeichen.
- enthält weniger als 1 Sonderzeichen.
- enthält weniger als 1 Großbuchstaben.
```

Verwendung durch den Endbenutzer oder Verwendung durch den Administrator

Endbenutzern und Tivoli-Administratoren, denen die Berechtigungsklasse **PasswordModifierRole** bzw. **user** zugeordnet ist, stehen für den Befehl **wpasswd** unterschiedliche Optionen zur Verfügung. Der Hauptunterschied besteht darin, dass Administratoren dazu berechtigt sind, Kennwörter anderer Benutzer zu ändern und Endbenutzer über diese Berechtigung nicht verfügen.

1. Administratoren können den Benutzernamen angeben, dessen Kennwörter geändert werden sollen. Endbenutzer können dies nicht tun, da sie nur Operationen ausführen dürfen, die sie selbst betreffen.
2. Die Identität von Endbenutzern wird überprüft, d. h., sie müssen ihre alten Kennwörter angeben. Die Identität von Administratoren wird anhand ihrer Tivoli-Berechtigungsklassen überprüft, so dass für Administratoren keine weitere Identitätsprüfung erforderlich ist. Administratoren müssen nicht das alte Kennwort des Benutzers, dessen Kennwort geändert wird, angeben.
3. Administratoren können Benutzerkennwörter ändern und den vorzeitigen Ablauf eines Benutzerkennworts festlegen, so dass sich der Benutzer zunächst mit dem neuen Kennwort anmelden kann, dieses jedoch sofort ändern muss. Da es für Endbenutzer keinen Sinn macht, für ihr eigenes Kennwort einen vorzeitigen Kennwortablauf festzulegen, steht diese Option Endbenutzern nicht zur Verfügung.

Verwendung auf verwalteten Knoten oder Verwendung auf TMA-Endpunkten

Bei der Installation von Tivoli SecureWay User Administration auf einem verwalteten Knoten wird auch der Befehl **wpasswd** installiert. Mit den Framework-Skripts **setup_env** werden die UNIX- bzw. NT-Umgebungsvariablen so angepasst, dass der Zugriff auf den

Befehl **wpasswd** möglich ist. Informationen zu den Adressen dieser Skripts auf den verschiedenen Systemarten finden Sie in der Framework-Dokumentation.

Die Installation des Befehls **wpasswd** auf einem TMA-Endpunkt erfolgt ini zwei Schritten. Zunächst muss das Gateway-Paket für Tivoli SecureWay User Administration auf allen Gateway-verwalteten Knoten installiert werden. Danach muss der Befehl **winstpw** ausgeführt werden, wobei die Namen der Endpunkte, auf denen der Befehl **wpasswd** ausgeführt werden soll, angegeben werden müssen. Mit den Framework-Skripts **lcf_env** werden die UNIX- bzw. NT-Umgebungsvariablen so angepasst, dass der Zugriff auf das Skript **wpasswd.sh** (**wpasswd.cmd** unter NT) möglich ist. Dieses Skript führt den Befehl **wpasswd** im Installationsverzeichnis aus, in dem es mit dem Befehl **winstpw** installiert wurde. Informationen zu den Adressen der Skripts **lcf_env** auf den verschiedenen Systemarten finden Sie in der Tivoli Management Framework-Dokumentation. Da Tivoli-Administratoren auf einem TMA-Endpunkt nicht eindeutig identifiziert werden können, können nur die für den Endbenutzer zur Verfügung stehenden Funktionen verwendet werden, wenn der Befehl wpasswd auf einem Endpunkt ausgeführt wird.

Tivoli Management Framework legt für Befehle wie **wpasswd** ein bestimmtes Zeitlimit fest, wann diese auf einem TMA-Endpunkt ausgeführt werden. Der Wert für dieses Zeitlimit, das so genannte Gateway-Zeitlimit, ist für die Ausführung von Befehlen der Art wie **wpasswd –L** möglicherweise zu niedrig. Aus diesem Grund gibt es für den Befehl **wpasswd** die Sonderoption **-T <Anzahl_Sekunden>**, die nur verfügbar ist, wenn der Befehl auf einem TMA-Endpunkt ausgeführt wird. Mit dieser Option können die Benutzer für das Gateway-Zeitlimit einen höheren Wert angeben, um sicher zu stellen, dass der Befehl vollständig ausgeführt wird.

Interne Informationen zum Befehl wpasswd

In den folgenden Abschnitten finden Sie interne Informationen zum Befehl **wpasswd**.

Gültigkeitsprüfung für alte Kennwörter

Das alte Kennwort, das vom Endbenutzer eingegeben wird, dient der Benutzeridentifikation. Für alle Benutzerdatensätze, in denen Benutzerkennwörter geändert werden, wird eine einzige Vergleichsoperation ausgeführt. Wenn das allgemeine Kennwort geändert wird, wird das allgemeine Kennwort, das im Benutzerdatensatz gespeichert ist, für den Vergleich herangezogen. Wenn das allgemeine Kennwort nicht geändert wird, wird für die Endpunktarten, deren Kennwörter geändert werden, das Endpunktartkennwort mit dem lexikalisch letzten Endpunktartcode für den Vergleich herangezogen. Dieser Vergleich muss für alle zu ändernden Kennwörter erfolgreich sein. Wenn dieser einzige Vergleich erfolgreich ist, werden keine weiteren Vergleiche durchgeführt. Bei Angabe der Option **–l** bzw. **–L** werden die alten Endpunktkennwörter nicht überprüft.

Leider gibt es keine Möglichkeit, die Identität eines Endbenutzers anhand eines weitergegebenen Benutzerdatensatzes zu überprüfen, es sei denn, der Benutzerdatensatz wurde von einem UNIX-System an einen UNIX-TMR-Server weitergegeben. Dies ist jedoch ein Sonderfall. Ein weitergegebener Benutzerdatensatz enthält niemals ein Kennwort in einem Format, das einen eindeutigen Vergleich ermöglicht. Nur eine Endpunktart, nämlich UNIX, gibt überhaupt bei einer Weitergabe ein Kennwort zurück. Das UNIX-Kennwort ist nach einem Einwegverschlüsselungsverfahren verschlüsselt. Nur auf einem UNIX-TMR- Server kann der Befehl **wpasswd** das alte Kennwort, das von einem Endbenutzer eingegeben wurde, nach UNIX-Standard verschlüsseln und die zwei verschlüsselten Kennwörter vergleichen. Auf allen anderen Servern ist diese Verschlüsselung nicht möglich.

Aus diesem Grund muss ein Tivoli-Administrator außer in reinen UNIX-TMRs manuell ein Kennwort in einen Benutzerdatensatz einfügen, damit Endbenutzer den Befehl **wpasswd** für dieses Kennwort ausführen können. Dem Administrator stehen hierfür zwei Möglichkeiten zur Verfügung: mit dem Befehl **wsetusr** wird nur der weitergegebene Datensatz modifiziert. Verwendet der Administrator den Befehl **wpasswd**, wird dasselbe Kennwort in alle Benutzerdatensätze des Endbenutzers eingefügt.

Verwendung der Option –L

Über die Option **–L** im Befehl **wpasswd** werden die modifizierten Benutzerdatensätze wieder in die Benutzerprofile eingefügt, bevor die Endpunktkennwörter aktualisiert werden. Wenn die Datensätze geschrieben werden, geht **wpasswd** davon aus, dass die Aktualisierung des Endpunkts erfolgreich ausgeführt wird, so dass CCMS dazu aufgefordert wird, die Uhrzeit, zu der der Benutzerdatensatz geändert wurde, nicht zu aktualisieren. Darüber hinaus werden die geänderten Hot Flags des Kennworts nicht in das Benutzerprofil eingefügt. Dies bedeutet, dass diese Datensätze erst bei der nächsten Verteilung zur "Profilpflege" verteilt werden, es sei denn, es werden vorher andere Änderungen an diesen Benutzerdatensätzen vorgenommen. Wenn vor der nächsten Verteilung zur "Profilpflege" andere Änderungen an diesen Datensätzen vorgenommen werden, werden diese Kennwortwerte von den empfangenden Endpunkten ignoriert.

Wenn die Kennwortänderung für Endpunkte über die Option **wpasswd –L** erfolgreich ausgeführt wird, treten keine Probleme auf. Eine unnötige Verteilung des Datensatzes wird vermieden und lokale Kennwortänderungen werden bei einer verzögerten Verteilung nicht von Kennwörtern, die mit einem Hot Flag versehen sind, überschrieben.

Wenn die Kennwortänderung für Endpunkte über die Option **wpasswd –L** fehlschlägt, treten jedoch Probleme auf. Wenn die Fehler behoben wurden, müssen Administratoren den Befehl **wsetusr** ausführen, um die Kennwörter des Benutzers in allen Benutzerdatensätzen des Benutzers explizit zu ändern, und dann diese Profile an die Endpunkte verteilen, auf denen der Befehl **wpasswd –L** fehlgeschlagen ist. Alternativ dazu kann nach der Fehlerbehebung erneut der Befehl **wpasswd –L** für diesen Benutzer bzw. von diesem Benutzer ausgegeben werden.

Verwendung von Mdist

Der Befehl **wpasswd –L** verwendet in Tivoli SecureWay User Administration Version 3.8 erstmals die Framework-Funktion **mdist**, um Endpunktkennwörter zeitgleich zu aktualisieren. Dadurch reduziert sich die Zeit, die für die Ausführung des Befehls **wpasswd –L** benötigt wird, erheblich. Da der Befehl **wpasswd –L** jedoch mit Vorsicht

eingesetzt werden muss, um unerwünschte Endpunktaktualisierungen zu vermeiden, ist der Zeitgewinn unterschiedlich groß. Wenn ein Benutzer Benutzerprofilen mehrerer Profilmanager zugeordnet ist, kann es sein, dass den verschiedenen Benutzerdatensätzen unterschiedliche Subskribenten zugeordnet sind. Ist dies der Fall, muss der Befehl **wpasswd –L** für jede Subskribentengruppe einen separaten **mdist**-Aufruf ausführen, so dass sich die Effektivität von **mdist** verringert.

Lange Kennwörter

Der Befehl **wpasswd** kann bei der Eingabe alter oder neuer Kennwörter bis zu 256 Zeichen lesen. Die Art des Systems, auf dem der Befehl ausgeführt wird, spielt dabei keine Rolle. Alle Kennwortqualitätsregeln werden jedoch nur auf die ersten N Zeichen dieser Zeichenfolge angewendet, wobei N die Anzahl der Zeichen ist, die in einem Kennwort einer Endpunktart, für die die Qualitätsregeln definiert wurden, maximal zulässig ist. Beispiel: wenn der Wert für die UNIX-Regel für die Mindestanzahl numerischer Zeichen (MinNumeric) 2 beträgt, müssen die ersten acht Zeichen der Kennwortzeichenfolge mindestens zwei numerische Zeichen enthalten. Die Länge der Zeichenfolge spielt dabei keine Rolle.

Anmerkung: Obwohl bis zu 256 Zeichen gelesen werden können, wird bei Angabe eines Kennworts, das mehr als 63 Zeichen enthält, die interne Verschlüsselung durch den Befehl **wpasswd** fehlschlagen. Die effektive maximale Länge für ein Kennwort in einem Tivoli SecureWay User Administration-Benutzerprofil beträgt 64 Zeichen.

Synchronisation von Tivoli ACF durch Tivoli SecureWay User Administration

Wenn Tivoli ACF mit Tivoli SecureWay User Administration Version 3.8 und Tivoli SecureWay Security Manager Version 3.7 eingesetzt werden, kann ACF die Gültigkeitsdauer von Kennwörtern auf UNIX-Systemen steuern, wenn alle Kennwortänderungen durch Tivoli SecureWay User Administration verwaltet werden. Tivoli ACF wird über alle Änderungen eines Benutzerkennworts auf einem UNIX-

System mit Tivoli ACF, die durch Tivoli SecureWay User Administration herbeigeführt wurden, informiert. Wenn Tivoli ACF feststellt, dass ein Kennwort abgelaufen ist, wird das neue Kennwort mit dem Befehl **wpasswdsync** abgerufen, so dass das neue Benutzerkennwort an Tivoli SecureWay User Administration und alle Subskribenten übermittelt wird. Diese Synchronisation erfolgt unabhängig davon, ob das UNIX-System von Tivoli SecureWay User Administration direkt oder indirekt, als NIS-Client eines von Tivoli SecureWay User Administration gesteuerten NIS-Servers, gesteuert wird.

Bei Verwaltung des Endpunkts durch Tivoli SecureWay User Administration

Die Synchronisation wird transparent ausgeführt, wenn der Endpunkt durch Tivoli SecureWay User Administration gesteuert wird. Wenn Tivoli SecureWay User Administration dazu aufgefordert wird, ein Benutzerkennwort auf einem UNIX-System zu ändern, überprüft es zunächst, ob Tivoli ACF auf dem System installiert ist. Wenn Tivoli ACF installiert und aktiviert ist, ändert Tivoli SecureWay User Administration das Benutzerkennwort und teilt Tivoli ACF mit, dass das Benutzerkennwort geändert wurde.

Wenn die Kennwortrichtlinie **UxPwMaxAge** von Tivoli SecureWay Security Manager an Tivoli ACF verteilt wurde, kann Tivoli ACF die Gültigkeitsdauer von Kennwörtern verwalten, sofern alle Kennwortänderungen von Tivoli SecureWay User Administration verwaltet werden. Auf UNIX-Systemen, auf denen die Tivoli SecureWay User Administration-Befehle **wpasswd** und **wpasswdsync** installiert sind, verwendet Tivoli ACF anstatt des Befehls **sepass** den Befehl **wpasswdsync**, um ein neues Benutzerkennwort abzurufen, wenn das aktuelle Kennwort abgelaufen ist und keine weiteren Anmeldungen für den Benutzer möglich sind. Mit dem Befehl **wpasswdsync**, der dem Befehl **wpasswd –L** entspricht, wird das neue Benutzerkennwort an Tivoli SecureWay User Administration und an alle subskribierenden Endpunkte übermittelt. Beachten Sie, dass der Befehl **winstpw –s** verwendet werden muss, wenn Tivoli ACF den Befehl **wpasswdsync** auf diese Weise auf einem Endpunkt des Tivoli-Verwaltungsagenten verwenden soll.

Bei Verwaltung des NIS-Servers durch Tivoli SecureWay User Administration

Bei NIS handelt es sich um eine Client-Pull-Technik, während Tivoli SecureWay User Administration eine Server-Push-Technik verwendet. Normalerweise ist NIS-Servern die Identität ihrer Clients unbekannt, oder sie ist für sie unerheblich. Bei Bedarf ruft jeder Client die benötigten Informationen vom Server dynamisch ab. Wenn jedoch Tivoli SecureWay User Administration und Tivoli ACF bezüglich Kennwortänderungen synchron laufen sollen, muss Tivoli SecureWay User Administration für alle NIS-Domänen, die es verwaltet, die UNIX-Systeme mit Tivoli ACF kennen, die Clients der jeweiligen NIS-Domäne sind.

Als Unterstützung hierfür hat Tivoli SecureWay User Administration Version 3.8 dem NIS-Objekt das Attribut Tivoli ACF Client Profile Manager hinzugefügt. Dieses Attribut wird über die Option **–C** *Profilmanager* in den Befehlen **wcrtdomain** und **wsetdomain** festgelegt. Alle Clients der NIS-Domäne, die Tivoli ACF verwenden und benachrichtigt werden möchten, wenn sich NIS-Kennwörter ändern, müssen Subskribenten dieses Profilmanagers sein. Wenn Tivoli SecureWay User Administration einem NIS-Objekt eine Kennwortänderung übermittelt, informiert das NIS-Objekt alle Endpunkte, die sich in der Subskriptionsbaumstruktur dieses Profilmanagers befinden über diese Änderung.

OnePassword

Tivoli SecureWay User Administration OnePassword ermöglicht Benutzern und Administratoren das Ändern von Benutzerkennwörtern in der TME-Datenbank sowie die Verteilung der aktualisierten Kennwörter an die zugeordneten Endpunkte. Dies geschieht über einen Web-Browser. Über eine zusätzliche Option können die Administratoren und Benutzer die aktualisierten Kennwörter entweder an alle oder an ausgewählte Endpunkte verteilen. Benutzer können über eine allgemeine OnePassword-Website ihre eigenen Kennwörter ändern. Authentifizierte Administratoren können auf der Website auch anderen Benutzern neue Kennwörter zuordnen.

Der Administrator kann nach erfolgter Authentifizierung beliebig viele Kennwortänderungen vornehmen. Die Authentifizierung läuft jedoch nach 60 Sekunden Inaktivität ab. Es wird aus Sicherheitsgründen empfohlen, dass der Administrator den Browser nach dem Ändern der Benutzerkennwörter schließt.

Der Benutzer bzw. Administrator verwendet OnePassword, indem er eine Verbindung zu einem Webserver herstellt, der sich auf dem TMR-Server befindet. Hier muss er einen Anmeldenamen und die zugehörigen Kennwörter angeben. Aus Sicherheitsgründen muss ein Benutzer sein altes und neues Kennwort eingeben. Ein Administrator muss zwar nur das neue Kennwort eingeben, muss für die Anmeldung jedoch eine Tivoli-Administrator-ID verwenden. OnePassword sucht anschließend in den Benutzerprofilen nach der Benutzer-ID. Stimmt das alte Kennwort mit dem allgemeinen Kennwort im Profil überein, ersetzt OnePassword das alte Kennwort durch das neue Kennwort für UNIX und NT und ersetzt das allgemeine Kennwort). Hierdurch werden die Kennwortattribute des Benutzers im entsprechenden Benutzerprofil aktualisiert. OnePassword verteilt das neue Kennwort im Benutzerprofil anschließend an alle zugeordneten Endpunkte.

Voraussetzungen für die Verwendung von OnePassword

Für die ordnungsgemäße Verwendung von OnePassword muss Javascript aktiviert sein. Sollte dies nicht so sein, ist die Weiterleitung bzw. Ausführung der HTML-Seiten von OnePassword nicht möglich. Bei Verwendung von Internet Explorer ist Javascript standardmäßig aktiviert. Falls Sie Netscape verwenden, müssen Sie folgende Schritte ausführen, um Javascript zu aktivieren:

Wählen Sie nacheinander die Optionen **Bearbeiten>Einstellungen>Erweitert>JavaScript aktivieren.**

Als Benutzer OnePassword verwenden

Als Benutzer können Sie auf die OnePassword-Website zugreifen und dort Ihre eigenen Kennwörter ändern.

Führen Sie folgende Schritte aus, um über OnePassword Ihre eigenen Kennwörter zu ändern:

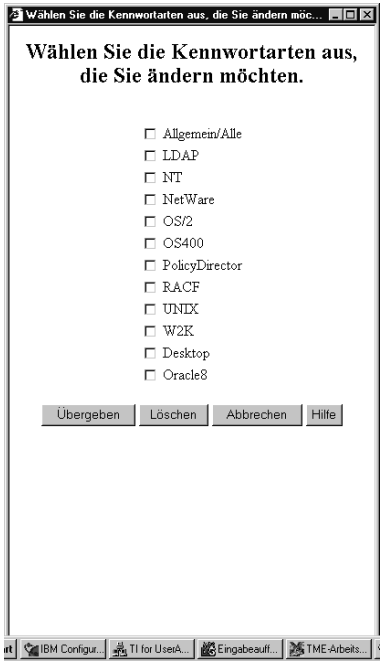
1. Öffnen Sie die Seite http://*HTTP-Server*/OnePassword.html

   HTTP-Server steht dabei für die URL des Webservers, der auf dem TMR-Server ausgeführt wird.

D:\IBM HTTP Server\htdocs\OnePassword.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address D:\IBM HTTP Server\htdocs\OnePassword.html
Go Links
Tivoli
OnePassword
Geben Sie Ihren Benutzernamen an:
Geben Sie Ihr altes Kennwort an:
Geben Sie Ihr neues Kennwort an:
Geben Sie Ihr neues Kennwort erneut an:
Wenn Sie alle Kennwörter ändern möchten, machen Sie die erforderlichen Angaben in den oben aufgeführten Textfeldern und klicken Sie anschließend auf diese Schaltfläche:
Alle Kennwörter ändern
Wenn Sie einige ausgewählte Kennwörter ändern möchten, machen Sie die erforderlichen Angaben in den oben aufgeführten Textfeldern und klicken Sie anschließend auf diese Schaltfläche:
Ausgewählte Kennwörter ändern
Löschen
Abbrechen
Hilfe
Letzte Änderung: 16. Mai 06:43:00 CST 2001
Done
My Computer

2. Geben Sie Folgendes ein:
   - Ihren Benutzernamen
   - Ihr altes Kennwort
   - Ihr neues Kennwort
   - Bestätigung des neuen Kennworts
3. Klicken Sie auf eine der folgenden Optionen:
   - **Alle Kennwörter ändern**
   - **Ausgewählte Kennwörter ändern**

Falls Sie **Ausgewählte Kennwörter ändern** ausgewählt haben, fahren Sie mit den Schritten 4 und 5 fort.



4. Wählen Sie aus, welche Kennwortart geändert werden soll.
5. Klicken Sie auf **Übergeben**.

Als Administrator OnePassword verwenden

Als Administrator können Sie über die OnePassword-Website die Kennwörter von Benutzern ändern.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklassen, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklassen
Als Administrator OnePassword verwenden	TMR	**admin** **Admin_Mod_Password**

Führen Sie folgende Schritte aus, um über OnePassword Benutzerkennwörter zu ändern:

1. Öffnen Sie die Seite http://*HTTP-Server*/OnePassword.html

   HTTP-Server steht dabei für die URL des Webservers, der auf dem TMR-Server ausgeführt wird.

D:\IBM HTTP Server\htdocs\OnePassword.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss
Address D:\IBM HTTP Server\htdocs\OnePassword.html
Go Links
Tivoli
OnePassword
Geben Sie Ihren Benutzernamen an:
Geben Sie Ihr altes Kennwort an:
Geben Sie Ihr neues Kennwort an:
Geben Sie Ihr neues Kennwort erneut an:
Wenn Sie alle Kennwörter ändern möchten, machen Sie die erforderlichen Angaben in den oben aufgeführten Textfeldern und klicken Sie anschließend auf diese Schaltfläche:
Alle Kennwörter ändern
Wenn Sie einige ausgewählte Kennwörter ändern möchten, machen Sie die erforderlichen Angaben in den oben aufgeführten Textfeldern und klicken Sie anschließend auf diese Schaltfläche:
Ausgewählte Kennwörter ändern
Löschen
Abbrechen
Hilfe
Letzte Änderung: 16. Mai 06:43:00 CST 2001
Done
My Computer

2. Geben Sie Folgendes ein:
   - Den Namen des Benutzers, dessen Kennwort geändert werden soll
   - Das neue Kennwort
   - Bestätigung des neuen Kennworts

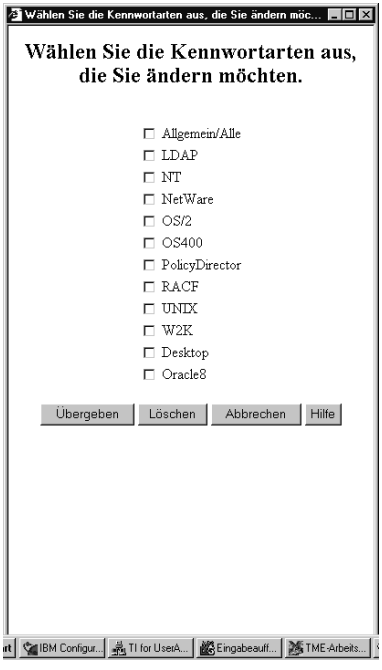
   Anmerkung: Durch das Leerlassen des Felds für das alte Kennwort identifizieren Sie sich gegenüber OnePassword als Tivoli-Administrator.

3. Klicken Sie auf eine der folgenden Optionen:
   - **Alle Kennwörter ändern**
   - **Ausgewählte Kennwörter ändern**

   Anmerkung: Da Sie sich als Tivoli-Administrator identifiziert haben, müssen Sie eine Authentifizierung vornehmen.

4. Geben Sie Folgendes ein:
   - Ihren Hostnamen (falls es sich nicht um die Maschine des TMR-Servers handelt).
   - Ihren Benutzernamen
   - Ihr Kennwort

   Falls Sie **Alle Kennwörter ändern** ausgewählt haben, fahren Sie mit den Schritten 5 und 6 fort.



5. Wählen Sie aus, welche Kennwortart geändert werden soll.
6. Klicken Sie auf **Übergeben**.

5

Benutzerprofile einrichten

Einführung

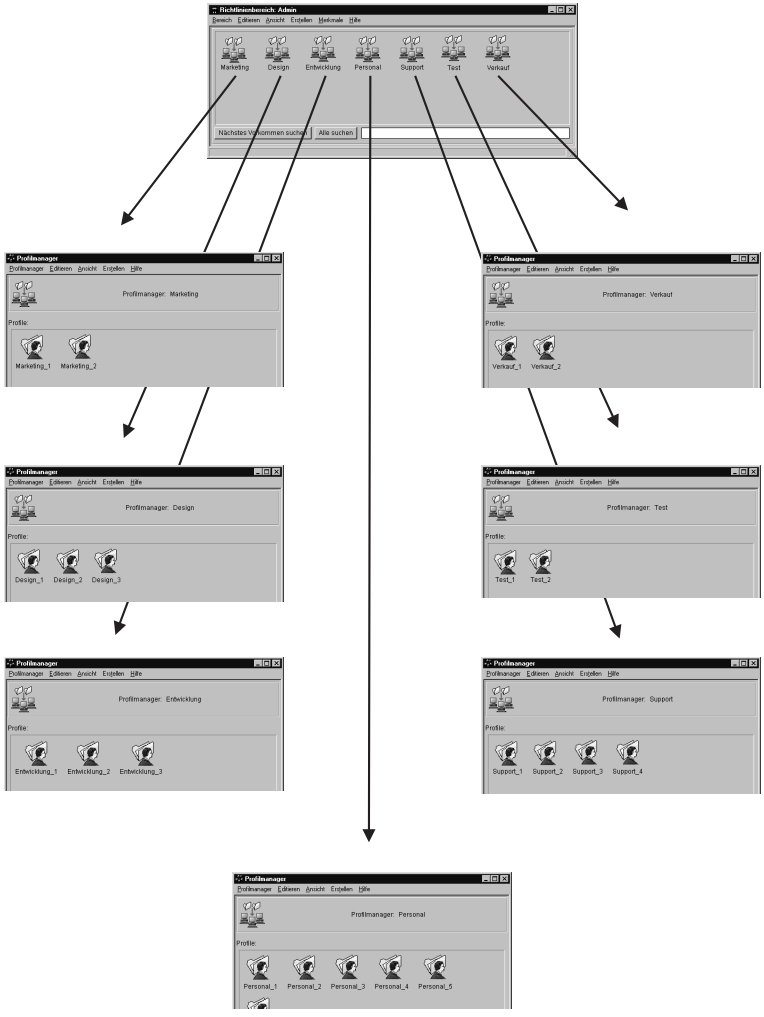
Da Sie wahrscheinlich eine große Anzahl Benutzer mit Tivoli SecureWay User Administration zu verwalten haben, müssen Sie Ihre Profile genau planen. Wenn Ihre Firma zum Beispiel 50.000 Benutzer hat, würde es sich nicht empfehlen, alle diese Benutzer in nur einem Benutzerprofil zu verwalten. Bei einer genauen Planung erhalten Sie Profilmanager und Profile, die leicht zu verwalten sind. Die NoonTide Corporation (eine fiktive Firma) hat beispielsweise 10.000 Mitarbeiter. In dieser Firma gibt es folgende Abteilungen: Marketing (Marketing), Verkaufsabteilung (Sales), Buchhaltung (Accounting), Personalabteilung (Human Resources), Unternehmensführung (Management), Entwicklungsabteilung (Development), Test (Testing), Design und Dokumentation (Design and Documentation), Kundenunterstützung (Customer Support) und interne Unterstützung (Internal Support).

In der folgenden Tabelle werden die Anzahl der Mitarbeiter jeder Abteilung, der Name des Profilmanagers, der der jeweiligen Abteilung zugeordnet ist, und die Profile, die jedem Profilmanager zugeordnet sind, aufgeführt:

Abteilung	**Anzahl der Mitarbeiter**	**Profil-managername**	**Profilnamen**
Design und Dokumentation	500	**Design**	**UI_design** **docs** **graphic_art**

Abteilung	Anzahl der Mitarbeiter	Profil-managername	Profilnamen
Entwicklung	2050	**Entwicklung**	**deadeye** **firestorm** **newcastle** **voyager**
Marketing	300	**Marketing**	**corporate** **region_1** **region_2** **region_3** **region_4**
Verkauf	3500	**Verkauf**	**sales_1** **sales_2** **sales_3** **sales_4**
Buchhaltung, Unternehmens-führung und Per-sonalabteilung	2250	**Personal**	**accounting** **human_resources** **management**
Test	400	**Test**	**test_dead** **test_fire** **test_new** **test_voyager**
Kundenunter-stützung und interne Unterstüt-zung	1000	**Support**	**external_1** **external_2** **external_3** **internal**

Betrachten Sie die folgende grafische Darstellung von Profilmanagern und den dort enthaltenen Profilen:



Zum Einrichten von Benutzerprofilen sollten Sie sich mit Profilmanagern, Profilen sowie mit Standardwertegruppen und Richtlinien für Gültigkeitsprüfung auskennen. Weitere Informationen finden Sie im *Tivoli Management Framework Benutzerhandbuch*.

Benutzerprofile einrichten

Ein Benutzerprofil enthält Benutzerdatensätze, die wiederum Benutzerinformationen enthalten. Jeder Benutzerdatensatz wird in einem plattformunabhängigen Format gespeichert, das die Verteilung derselben Profildatensätze in einer Umgebung mit mehreren Plattformen ermöglicht.

Jedes Benutzerprofil enthält eine Reihe von Standardwertegruppen und Richtlinien für Gültigkeitsprüfung. Standardwertegruppen legen Standardwerte fest, die verwendet werden, wenn Sie einen neuen Profildatensatz erstellen. Richtlinien für Gültigkeitsprüfung definieren zulässige Werte für die Optionen in einem Profildatensatz.

Anmerkung: Beachten Sie, dass Tivoli SecureWay User Administration profilbasierte und keine regionsbasierten Richtlinien verwendet.

Benutzerprofile als verwaltete Ressourcen zuordnen

Jeder Richtlinienbereich unterhält eine Liste mit verwalteten Ressourcenarten, die für den spezifischen Richtlinienbereich gültig sind oder definiert wurden. Sie müssen Benutzerprofile als verwaltete Ressourcen hinzufügen, bevor Sie einen Richtlinienbereich für die Verwaltung von Benutzern verwenden können.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Benutzerprofile als verwaltete Ressourcen für einen Richtlinienbereich hinzufügen	Richtlinienbereich	**senior**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Benutzerprofile als verwaltete Ressourcen für den Richtlinienbereich hinzuzufügen:

1. Klicken Sie in der Liste **Verfügbare Ressourcen** doppelt auf die Option **UserProfile**. Dadurch wird die ausgewählte verwaltete Ressource in die Liste **Aktuelle Ressourcen** verschoben.
2. Klicken Sie auf **Festlegen und schließen**, um die neue verwaltete Ressource dem Richtlinienbereich hinzuzufügen, und schließen Sie den Dialog **Verwaltete Ressourcen festlegen**.

Befehlszeile

Im folgenden Beispiel werden Benutzerprofile als verwaltete Ressourcen dem Richtlinienbereich hinzugefügt:

```
wsetpr UserProfile @PolicyRegion:Noon-region
```

Dabei gilt Folgendes:

UserProfile
: Gibt die verwaltete Ressourcenart an, die dem Richtlinienbereich hinzugefügt werden soll.

@PolicyRegion:Noon-region
: Gibt den Namen des Richtlinienbereichs an.

Weitere Informationen zur Verwendung der Befehlszeile, um einem Richtlinienbereich Benutzerprofile als verwaltete Ressourcen hinzuzufügen, finden Sie im Abschnitt zum Befehl **wsetpr** des Handbuchs *Tivoli Framework Reference Manual*.

Benutzerprofile erstellen

Zum Verwalten von Benutzerkonten mit Tivoli SecureWay User Administration müssen Sie zuerst ein Benutzerprofil erstellen. Je nachdem, wie viele Benutzer Sie zu verwalten haben, könnte es sich empfehlen, mehr als ein Benutzerprofil zu erstellen. Ein Benutzerprofil enthält zunächst keine Datensätze, es enthält jedoch eine Reihe von Standardwertegruppen und Richtlinien für Gültigkeitsprüfung, die von Tivoli bereitgestellt werden.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

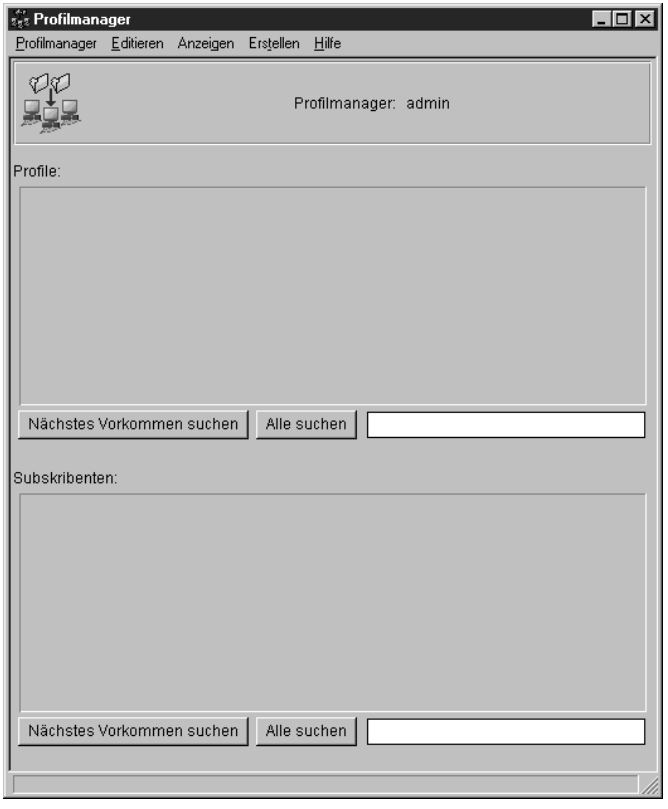
Aktivität	Umgebung	Berechtigungsklasse
Benutzerprofil erstellen	Profilmanager	**senior**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

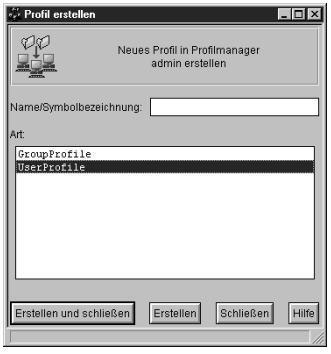
Arbeitsoberfläche

Führen Sie folgende Schritte aus, um ein Benutzerprofil zu erstellen:

1. Klicken Sie im Richtlinienbereich doppelt auf das Symbol eines Profilmanagers, um das Fenster **Profilmanager** anzuzeigen.



2. Wählen Sie im Menü **Erstellen** die Option **Profil** aus, um den Dialog **Profil erstellen** anzuzeigen.



3. Geben Sie einen eindeutigen Namen für das Profil im Feld **Name/Symbolbezeichnung** ein.

   Anmerkung: Ein Profilname darf in der TMR nicht doppelt vorkommen.

4. Wählen Sie **UserProfile** in der Liste **Art** aus.
5. Klicken Sie auf **Erstellen und schließen**, um das Profil zu erstellen und zum Fenster **Profilmanager** zurückzukehren.

Tivoli SecureWay User Administration erstellt das Benutzerprofil und zeigt im Fenster **Profilmanager** das Symbol des Profils an.

Befehlszeile

Im folgenden Beispiel wird ein Benutzerprofil erstellt:

```
wcrtprf @ProfileManager:marketing UserProfile corporate
```

Dabei gilt Folgendes:

@ProfileManager:marketing
: Gibt den Namen des Profilmanagers an, in dem das Profil erstellt werden soll.

UserProfile
: Gibt die zu erstellende Profilart an.

corporate
Gibt den Namen des neuen Benutzerprofils an.

Informationen zum Erstellen eines Benutzerprofils mit Hilfe der Befehlszeile finden Sie in der Beschreibung des Befehls **wcrtprf** im Handbuch *Tivoli Framework Reference Manual*.

Benutzerprofile klonen

Beim Klonen eines Benutzerprofils wird eine Kopie des Profils, einschließlich der Standardwertegruppen und Richtlinien für Gültigkeitsprüfung, erstellt, allerdings ohne Datensätze.

Anmerkung: Tivoli AEF (Tivoli Application Extension Facility) kann zum Erstellen von Attributen, Anpassen von Dialogen oder bei Statusänderungen von Benutzerdatensätzen zum Ausführen von Skripts eingesetzt werden. Beim Klonen eines Benutzerprofils, an dem Anpassungen über AEF vorgenommen wurden, wird ein Profil mit den angepassten Attributen und Skripts, jedoch ohne die Dialoganpassungen erstellt.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

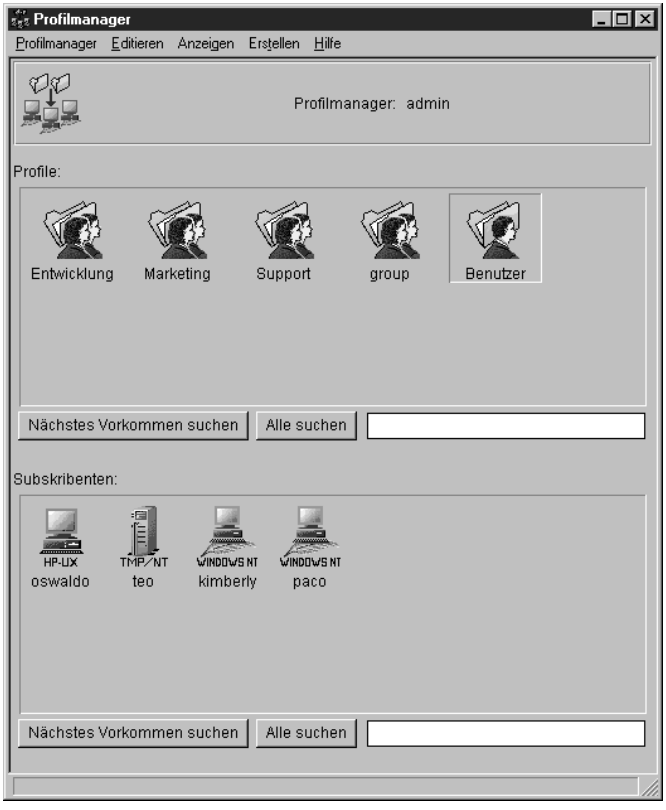
Aktivität	Umgebung	Berechtigungsklasse
Benutzerprofil klonen	Profilmanager	**senior**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um ein Benutzerprofil zu klonen:

1. Klicken Sie in einem Richtlinienbereich doppelt auf das Symbol eines Profilmanagers, um das Fenster **Profilmanager** anzuzeigen.



2. Wählen Sie das Symbol des zu klonenden Profils aus.

3. Wählen Sie im Menü **Editieren** die Optionen **Profile –> Klonen** aus, um den Dialog **Profil klonen** anzuzeigen.

4. Geben Sie den Namen des neuen Profils im Feld **Name/Symbolbezeichnung** ein.
5. Klicken Sie auf **Klonen und schließen**, um das ausgewählte Profil zu klonen und zum Fenster **Profilmanager** zurückzukehren.

Tivoli SecureWay User Administration erstellt das neue Profil mit allen Standardwertegruppen und Richtlinien des geklonten Profils.

Befehlszeile

Im folgenden Beispiel wird ein Benutzerprofil geklont:

```
wcrtprf -c @UserProfile:region_1 \
@ProfileManager:marketing UserProfile region_2
```

Dabei gilt Folgendes:

-c Gibt das zu klonende Benutzerprofil an.

@UserProfile:region_1
Gibt den Namen des Quellenprofils an.

@ProfileManager:marketing
Gibt den Profilmanager an, in dem das neue Profil erstellt wird.

UserProfile
Gibt die zu erstellende Profilart an.

region_2
Gibt den Namen des neuen Profils an.

Informationen zum Klonen eines Benutzerprofils mit Hilfe der Befehlszeile finden Sie in der Beschreibung des Befehls **wcrtprf** im Handbuch *Tivoli Framework Reference Manual*.

Benutzerprofile löschen

Anmerkung: Durch Löschen eines Benutzerprofils werden nicht die Systembenutzerinformationen auf den Subskriptionsendpunkten gelöscht.

Durch Löschen eines Benutzerprofils werden das ursprüngliche Profil und seine Datensätze aus dem Profilmanager gelöscht. Es werden außerdem Kopien des Profils aus den Subskribenten des Profilmanagers gelöscht. Zum Löschen der Systembenutzerinformationen auf den Subskriptionsendpunkten müssen Sie die Datensätze aus dem Profil löschen und dieses anschließend an die Endpunkte verteilen. Ein zum Löschen markierter Benutzerdatensatz wird aus den Endpunkten entfernt, an die das Benutzerprofil verteilt wird.

Wenn Sie alle zuvor im Profil definierten Informationen löschen und dieses Profil verteilen, werden alle Benutzer aus den Endpunkten entfernt, an die dieses Benutzerprofil verteilt wird. Ausnahmen sind der Eintrag **root** und alle NIS-Anweisungen in den Konfigurationsdateien auf einem UNIX-Endpunkt, der Eintrag **Administrator** auf einem Windows NT-Endpunkt sowie der Eintrag 'Admin' auf einem NetWare-Endpunkt. Eine vollständige Liste der geschützten Konten finden Sie im Handbuch *Tivoli SecureWay User Administration Reference Manual.*

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

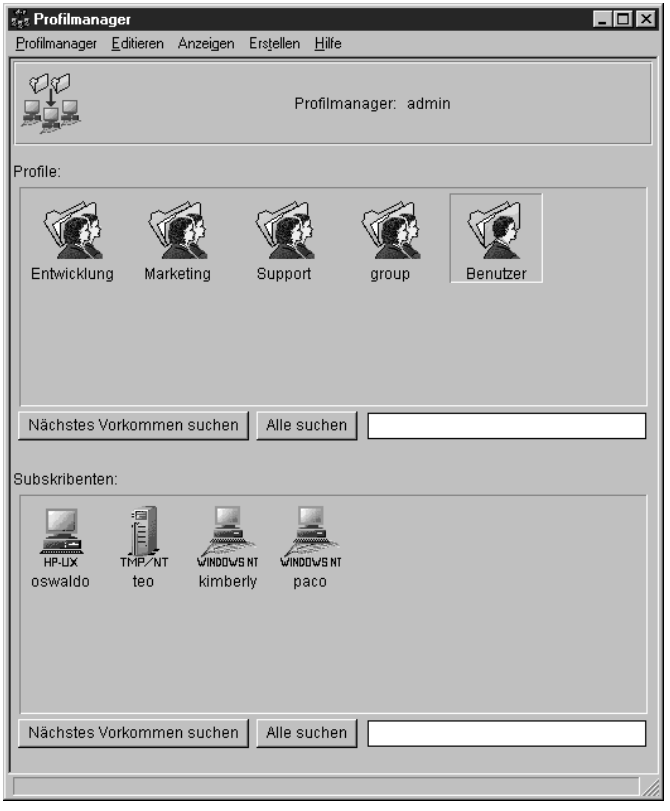
Aktivität	Umgebung	Berechtigungsklasse
Benutzerprofil löschen	Profilmanager	**senior**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um ein Benutzerprofil zu löschen:

1. Klicken Sie in einem Richtlinienbereich doppelt auf das Symbol eines Profilmanagers, um das Fenster **Profilmanager** anzuzeigen.



2. Wählen Sie das zu löschende Benutzerprofil aus.

3. Wählen Sie **Profile –> Löschen** im Menü **Editieren** aus, um einen Bestätigungsdialog anzuzeigen.

4. Klicken Sie auf **Löschen**, um das Profil zu löschen und zum Fenster **Profilmanager** zurückzukehren.

Tivoli SecureWay User Administration löscht das Profil und dessen Kopien aus den zugeordneten Profilmanagern.

Befehlszeile

Im folgenden Beispiel wird ein Benutzerprofil gelöscht:

```
wdel @UserProfile:region_5
```

Dabei gilt Folgendes:

@UserProfile:region_5
Gibt das zu löschende Benutzerprofil an.

Informationen zum Löschen eines Benutzerprofils über die Befehlszeile finden Sie in der Beschreibung des Befehls **wdel** im Handbuch *Tivoli Framework Reference Manual*.

Mit Richtlinien für Benutzerprofile arbeiten

Jedes Benutzerprofil enthält eine Reihe von Standardwertegruppen und Richtlinien für Gültigkeitsprüfung. Standardwertegruppen legen die Standardwerte fest, die verwendet werden, wenn Sie einen neuen Profildatensatz erstellen. Richtlinien für Gültigkeitsprüfung legen die zulässigen Werte für die Attribute von Profildatensätzen fest.

Standardwertegruppen definieren

Jedes Benutzerprofil besitzt eine Reihe von Standardwertegruppen. Es gibt eine Standardwertegruppe für die meisten Attribute, die einem Benutzerdatensatz zugeordnet sind. Durch das Definieren dieser Standardwertegruppen erstellen Sie eine Schablone für jeden neuen Datensatz, der dem Profil hinzugefügt wird. Mit dieser Schablone müssen Sie nur ein Minimum an Informationen eingeben, um einen vollständigen Benutzerdatensatz zu erstellen. Wenn Sie Informationen in den Benutzerdatensatz eingeben und anschließend auf **Standardeinstellungen generieren** oder auf **Hinzufügen** klicken, übernimmt Tivoli SecureWay User Administration für alle Attribute, für die Sie keinen Wert eingegeben haben, die Werte aus der definierten Standardwertegruppe. .

Anmerkung: Für die Weitergabe von Daten an NetWare-Benutzer müssen Sie unter Umständen die Standardwertegruppen **nw_nds_context** und **nw_volume_restrictions** zurücksetzen. Weitere Informationen hierzu finden Sie unter „Daten an Benutzerprofile weitergeben” auf Seite 144 und im Kapitel über Richtlinien im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

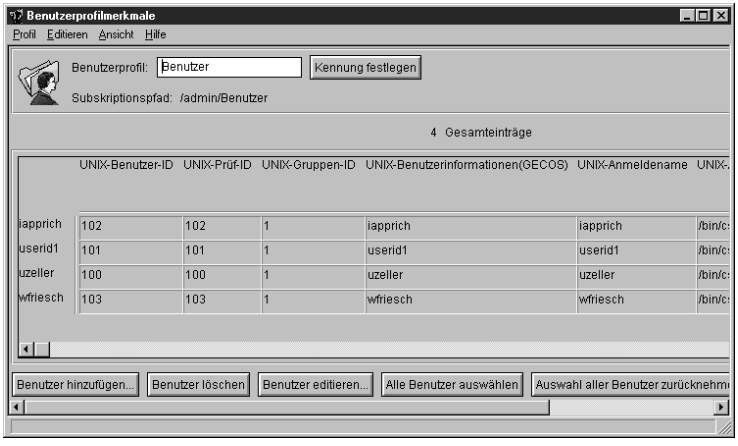
Aktivität	Umgebung	Berechtigungsklasse
Standardwertegruppe für Benutzer editieren	Benutzerprofil	**senior**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

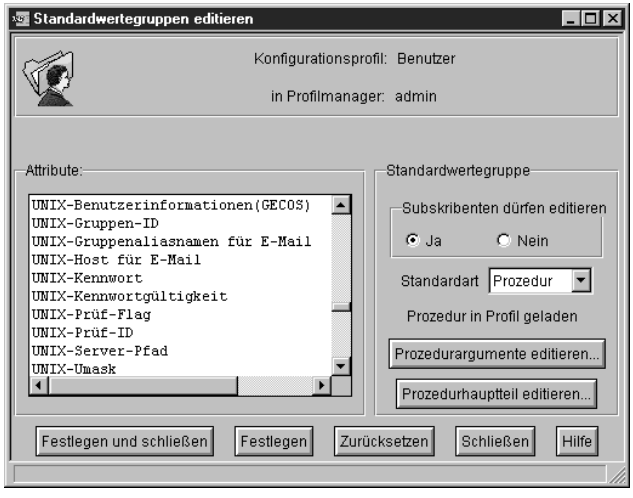
Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Standardwertegruppen für Benutzer zu editieren:

1. Klicken Sie doppelt auf das Symbol eines Benutzerprofils, um das Fenster **Benutzerprofilmerkmale** anzuzeigen.



2. Wählen Sie **Standardwertegruppen** im Menü **Editieren** aus, um den Dialog **Standardwertegruppen editieren** anzuzeigen.



3. Wählen Sie ein Attribut in der Liste **Attribute** aus.
4. Klicken Sie auf das Optionsfeld **Ja** im Feld **Subskribenten dürfen editieren**, damit Subskribenten Änderungen durchführen können. Klicken Sie andernfalls auf das Optionsfeld **Nein**.

5. Wählen Sie eine Standardart in der Dropdown-Liste **Standardart** aus. Die verfügbaren Optionen lauten: **Keine**, **Konstante** oder **Skript** (früher: Prozedur).

   Wenn Sie die Option **Konstante** auswählen, geben Sie einen konstanten Wert in das Feld **Wert** ein.

   Führen Sie folgende Schritte aus, wenn Sie die Option **Skript** ausgewählt haben:

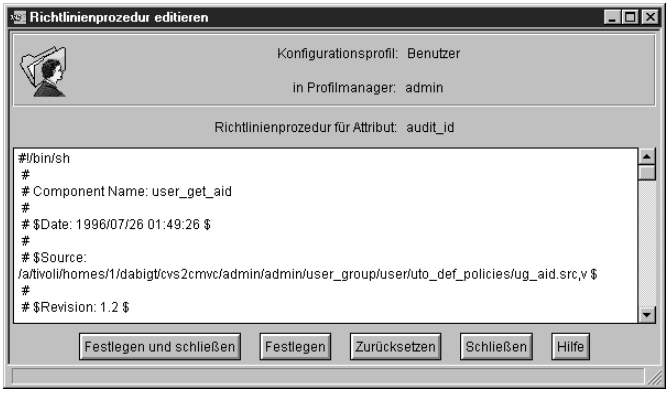
   a. Klicken Sie auf **Skriptargumente editieren...** (früher: Prozedurargumente editieren...), um den Dialog **Argumente des Richtlinienskripts** (früher: Argumente der Richtlinienprozedur) anzuzeigen. Bestimmen Sie in diesem Dialog die Reihenfolge der Skriptargumente.

   b. Wählen Sie in der Liste **Attribute** die Attribute aus, die Sie als Skriptargumente für das Richtlinienskript des aktuellen Attributs verwenden möchten. Klicken Sie auf den Rechtspfeil, um die Attribute in die Liste **Skriptargumente** (früher: Prozedurargumente) zu verschieben.

      Sie können die Reihenfolge der Argumente für eine Richtlinie ändern, indem Sie das Argument auswählen und auf den Aufwärtspfeil bzw. den Abwärtspfeil klicken, um das Argument an die gewünschte Position zu verschieben.

   c. Klicken Sie auf **Festlegen und schließen**, um die neuen Argumente hinzuzufügen und zum Dialog **Standardwertegruppen editieren** zurückzukehren.

d. Klicken Sie auf **Skripthauptteil editieren...** (früher: Prozedurhauptteil editieren...) im Dialog **Standardwertegruppen editieren**, um den Dialog **Richtlinienskript editieren** (früher: Richtlinienprozedur editieren)anzuzeigen.



e. Bearbeiten Sie den Hauptteil des Skripts.

f. Klicken Sie auf **Festlegen und schließen**, um das Skript in der Datenbank zu speichern und zum Dialog **Standardwertegruppen editieren** zurückzukehren.

   Wiederholen Sie diesen Vorgang für jedes Attribut des Datensatzes.

g. Klicken Sie auf **Festlegen und schließen**, um die Änderungen anzuwenden und zum Fenster **Benutzerprofilmerkmale** zurückzukehren.

Befehlszeile

Um die Standardwertegruppen für ein Benutzerprofil über die Befehlszeile festzulegen, können Sie die Attributnamen in einem angegebenen Profil zuerst mit dem Befehl **wlspolm** auflisten. Mit dem Befehl **wgetpolm** legen Sie dann die aktuelle Standardwertegruppe für ein angegebenes Attribut fest. Anschließend können Sie mit dem Befehl **wputpolm** die Standardwertegruppe für das Attribut ändern.

Im folgenden Beispiel werden die Attribute für ein Benutzerprofil aufgelistet:

```
wlspolm @UserProfile:corporate
```

Dabei gilt Folgendes:

@UserProfile:corporate: Gibt den Namen des Profils an, dessen Attribute aufgelistet werden sollen.

Befehlsausgabe:

```
real_name
login_name
password
passwd_aging
...
```

Im folgenden Beispiel wird die momentan definierte Standardwertegruppe für ein angegebenes Attribut des Benutzerprofils zurückgegeben:

```
wgetpolm -d @UserProfile:corporate gid
```

Im folgenden Beispiel wird die Standardwertegruppe für ein Benutzerprofil gesetzt:

```
wputpolm -d -c 10 @UserProfile:corporate gid
```

Dabei gilt Folgendes:

-d Setzt die Standardwertegruppe.

-c 10 Gibt 10 als den konstanten Wert für die neue Standardwertgruppe an.

@UserProfile:corporate
Gibt den Namen des Profils an, für das eine Richtlinie gesetzt werden soll.

gid Gibt das Attribut an, für das eine Richtlinie gesetzt wird.

Informationen zum Editieren von Standardwertegruppen mit Hilfe der Befehlszeile finden Sie in der Beschreibung der Befehle **wgetpolm**, **wputpolm** und **wlspolm** im Handbuch *Tivoli Framework Reference Manual*.

Anmerkung: Die Richtlinie für jedes Profilattribut wird in dem entsprechenden Attributsegment in einem speziellen Datensatz für das Attribut, im Standarddatensatz und im Prüfdatensatz gespeichert. Wenn Sie beispielsweise das ursprüngliche Skript für die Standardrichtlinie der Gruppen-ID durch eine Konstante ersetzen und anschließend die Richtlinienart wieder in das Skript ändern, so steht der Inhalt des ursprünglichen Skripts nicht mehr zur Verfügung. Sie können jedoch dieses Skript aus einem unveränderten Profil extrahieren und damit den ursprünglichen Inhalt wiederherstellen.

Plattformspezifische Standardwertegruppen inaktivieren

Tivoli SecureWay User Administration stellt Standardwertegruppen-Skripts für UNIX, NetWare, Windows NT und Windows 2000-Benutzerkonten bereit. Wenn Sie ein neues Benutzerkonto erstellen, definiert die Anwendung standardmäßig Attribute für alle drei Plattformtypen. Wenn Ihre Netzwerkumgebung einen oder mehrere dieser Plattformtypen nicht enthält, dann wird der Prozess zum Erstellen eines neuen Benutzers unnötig verlangsamt. Wenn Sie zum Beispiel NetWare nicht verwenden, können Sie die Standardwertegruppen für NetWare inaktivieren. Folglich wird die zum Erstellen eines Benutzers benötigte Zeit geringer, da die Skripts für die Standardwertegruppen für NetWare nicht im Hintergrund ausgeführt werden.

Mit dem Befehl **wsetdefpol** können Sie die plattformspezifischen Standardwertegruppen eines vorgegebenen Benutzerprofils inaktivieren bzw. aktivieren. Wenn Sie **TivoliDefaultUserProfile** als Profilnamen angeben, erbt jedes Benutzerprofil, das nach Ausführung des Befehls **wsetdefpol** erstellt wurde, die angegebenen Einstellungen der Standardwertegruppe.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Standardwertegruppe für eine Plattform inaktivieren	Benutzerprofil	**keine**

Sie können diese Task nur über die Befehlszeile ausführen.

Im folgenden Beispiel wird die Standardwertegruppe für NetWare inaktiviert:

```
wsetdefpol DISABLED NW corp-users
```

Dabei gilt Folgendes:

DISABLED
Gibt an, dass die Standardwertegruppe inaktiviert werden soll.

NW Gibt an, dass die NetWare-spezifische Richtlinie inaktiviert werden soll.

corp-users
Gibt das Benutzerprofil an.

Informationen zum Aktivieren und Inaktivieren plattformspezifischer Standardwertegruppen über die Befehlszeile finden Sie in der Beschreibung des Befehls **wsetdefpol** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Richtlinien für Gültigkeitsprüfung definieren

Benutzerprofile können ausgewertet werden, um sicherzustellen, dass die einem Profildatensatz hinzugefügten Informationen den aktuellen Richtlinienregeln entsprechen. Der Profildatensatz für Gültigkeitsprüfung gibt die beim Hinzufügen eines neuen Profildatensatzes oder beim Ändern eines vorhandenen Datensatzes verwendeten Richtlinien für Gültigkeitsprüfung an.

Eine Beschreibung der von Tivoli zur Verfügung gestellten Richtlinien für Gültigkeitsprüfung finden Sie im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

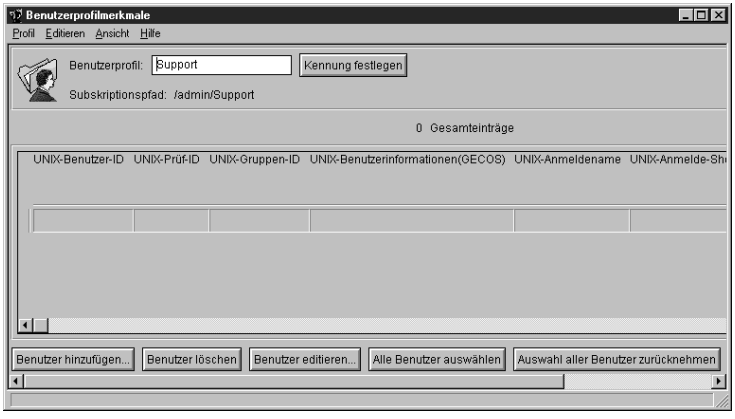
Aktivität	Umgebung	Berechtigungsklasse
Richtlinien für Gültigkeitsprüfung von Benutzern editieren	Benutzerprofil	**senior**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

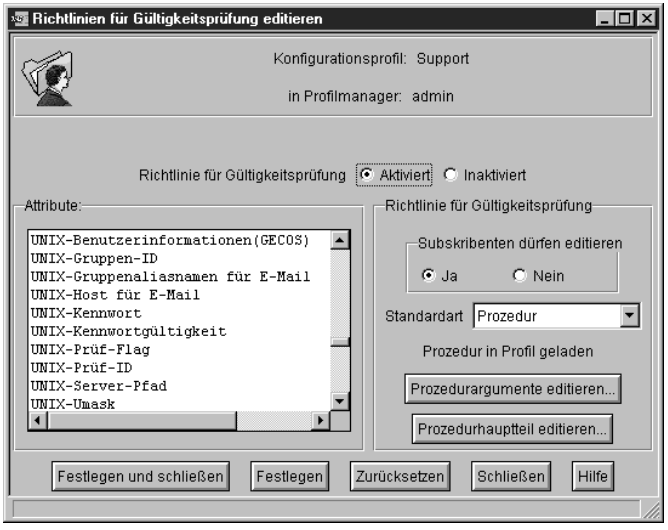
Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Richtlinien für Gültigkeitsprüfung zu editieren:

1. Klicken Sie doppelt auf das Symbol eines Benutzerprofils, um das Fenster **Benutzerprofilmerkmale** anzuzeigen.



2. Wählen Sie **Richtlinien für Gültigkeitsprüfung** im Menü **Editieren** aus, um den Dialog **Richtlinien für Gültigkeitsprüfung editieren** anzuzeigen.



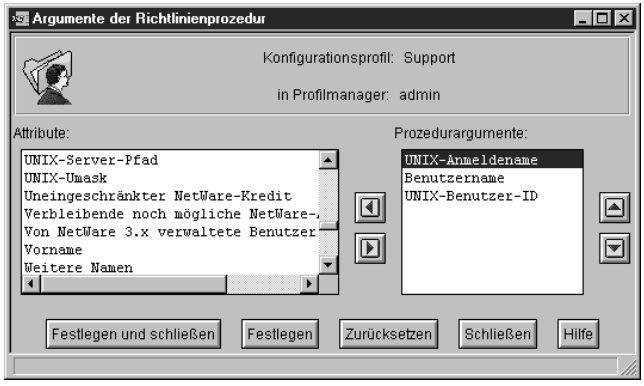
3. Wählen Sie ein Attribut in der Liste **Attribute** aus.
4. Klicken Sie auf das Optionsfeld **Ja** im Feld **Subskribenten dürfen editieren**, damit Subskribenten diese Richtlinie ändern können; klicken Sie andernfalls auf das Optionsfeld **Nein**.
5. Wählen Sie in der Dropdown-Liste **Standardart** eine Gültigkeitsart aus. Die verfügbaren Optionen lauten: **Keine**, **Konstante**, **Skript** (früher: Prozedur) und **Regulärer Ausdruck**.

   Wenn Sie die Option **Konstante** auswählen, geben Sie einen konstanten Wert in das Feld **Wert** ein.

   Wenn Sie **Regulärer Ausdruck** auswählen, geben Sie einen regulären Perl-Ausdruck in das Feld **Wert** ein.

   Führen Sie folgende Schritte aus, wenn Sie die Option **Skript** ausgewählt haben:

   a. Klicken Sie auf **Skriptargumente editieren...** (früher: Prozedurargumente editieren...), um den Dialog **Argumente des Richtlinienskripts** (früher: Argumente der Richtlinienprozedur) anzuzeigen. Bestimmen Sie in diesem Dialog die Reihenfolge der Skriptargumente.

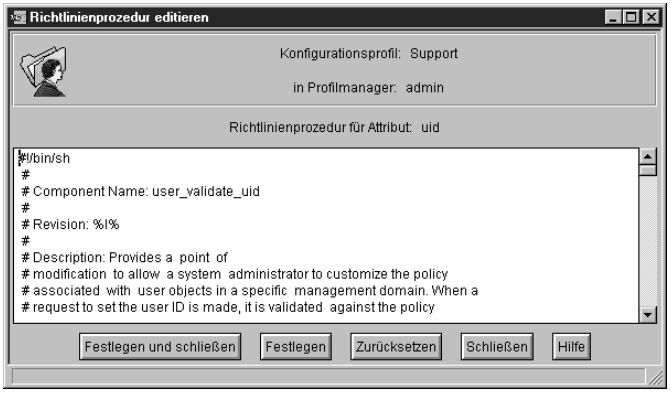


b. Wählen Sie in der Liste **Attribute** die Attribute aus, die Sie als Skriptargumente für das Richtlinienskript des aktuellen Attributs verwenden möchten. Klicken Sie auf den Rechtspfeil, um die Attribute in die Liste **Skriptargumente** (früher: Prozedurargumente) zu verschieben.

   Sie können die Reihenfolge ändern, in der ein Argument aufgerufen wird, indem Sie das Argument auswählen und auf den Aufwärtspfeil bzw. den Abwärtspfeil klicken, um das Argument an die gewünschte Position zu verschieben.

c. Klicken Sie auf **Festlegen und schließen**, um die neuen Argumente hinzuzufügen und zum Dialog **Richtlinien für Gültigkeitsprüfung editieren** zurückzukehren.

d. Klicken Sie auf **Skripthauptteil editieren...** (früher: Prozedurhauptteil editieren...) im Dialog **Richtlinien für Gültigkeitsprüfung editieren**, um den Dialog **Richtlinienskript editieren** (früher: Richtlinienprozedur editieren) anzuzeigen.



e. Bearbeiten Sie den Hauptteil des Skripts.

f. Klicken Sie auf **Festlegen und schließen**, um das Skript in der Datenbank zu speichern und zum Dialog **Richtlinien für Gültigkeitsprüfung editieren** zurückzukehren.

   Wiederholen Sie diesen Vorgang für jedes Attribut des Datensatzes.

6. Klicken Sie auf **Festlegen und schließen**, um die Änderungen anzuwenden und zum Fenster **Benutzerprofilmerkmale** zurückzukehren.

Befehlszeile

Um die Richtlinien für Gültigkeitsprüfung für ein Benutzerprofil über die Befehlszeile zu setzen, können Sie die Attributtypen in einem angegebenen Profil zuerst mit dem Befehl **wlspolm** auflisten. Mit dem Befehl **wgetpolm** legen Sie dann die aktuelle Standardwertegruppe für ein angegebenes Attribut fest. Anschließend können Sie mit dem Befehl **wputpolm** die Standardwertegruppe für das Attribut ändern.

Im folgenden Beispiel werden die Attribute für ein Benutzerprofil aufgelistet:

```
wlspolm @UserProfile:firestorm
```

Dabei gilt Folgendes:

@UserProfil:firestorm: Gibt den Namen des Profils an, dessen Attribute aufgelistet werden sollen.

Befehlsausgabe:

```
real_name
login_name
password
passwd_aging
...
```

Im folgenden Beispiel wird die momentan definierte Richtlinie für Gültigkeitsprüfung für ein angegebenes Attribut des Benutzerprofils zurückgegeben:

```
wgetpolm -v @UserProfile:firestorm gid
```

Im folgenden Beispiel wird die Gültigkeitsprüfung für ein Benutzerprofil inaktiviert. Es wird darauf hingewiesen, dass das Attribut einen beliebigen Wert annehmen kann:

```
wputpolm -v -n @UserProfile:firestorm gid
```

Dabei gilt Folgendes:

-v Setzt die Richtlinie für Gültigkeitsprüfung fest.

-n Inaktiviert die Gültigkeitsprüfung für das angegebene Attribut.

@UserProfile:firestorm
Gibt den Namen des Profils an, für das eine Richtlinie gesetzt werden soll.

gid Gibt das Attribut an, für das eine Richtlinie gesetzt wird.

Informationen zum Editieren der Richtlinien für Gültigkeitsprüfung von Benutzern mit Hilfe der Befehlszeile finden Sie in der Beschreibung der Befehle **wgetpolm**, **wputpolm** und **wlspolm** im Handbuch *Tivoli Framework Reference Manual*.

Benutzerprofile verwalten

Sobald Sie die Benutzerprofile erstellt und die Standardwertegruppen und Richtlinien für Gültigkeitsprüfung festgelegt haben, müssen Sie die Benutzerdatensätze hinzufügen. Eine Möglichkeit, wie Sie Benutzerdatensätze schnell hinzufügen, besteht darin, von den Subskribenten aus Benutzerinformationen an das Benutzerprofil weiterzugeben. Eine weitere Task, die Sie ausführen müssen, ist das Festlegen der Standardwerte für die Verteilung des Profils.

Daten an Benutzerprofile weitergeben

Sobald Sie die Benutzerprofile erstellt und die Standardwertegruppen und Richtlinien für Gültigkeitsprüfung festgelegt haben, können Sie vorhandene Benutzerkontoinformationen an die Benutzerprofile weitergeben (d. h. können Sie Benutzerprofile mit Benutzerkontoinformationen füllen). Durch die Datenweitergabe werden Benutzerinformationen von den angegebenen Endpunkten in die Benutzerdatensätze des aktuellen Benutzerprofils importiert.

Wenn Sie die Zusammenfügungsoption des Befehls **wpopusrs** verwenden, versucht Tivoli SecureWay User Administration, die Benutzerinformationen aus der verwalteten Ressource und die Benutzerdatensätze im Profil zusammenzufügen. Übereinstimmungen werden dabei anhand des **Anmeldenamens** festgestellt. Wenn eine Übereinstimmung gefunden wird, vergleicht Tivoli SecureWay User Administration die Betriebssystemkontoarten. Wenn diese unterschiedlich sind, fügt die Anwendung die Informationen in dem Datensatz zusammen. Sind sie identisch, gibt Tivoli SecureWay User Administration einen Fehler zurück.

Wenn die Benutzerinformationen mit einem Benutzerdatensatz zusammengefügt werden, werden die neuen Benutzerinformationen in den Benutzerdatensatz aufgenommen, und die allgemeinen Benutzerinformationen werden auf Attributbasis mit den Informationen zusammengefügt, die in dem Benutzerdatensatz vorhanden sind, der Vorrang hat.

Es gibt zum Beispiel einen Datensatz im Profil, in dem **freddie** als Anmeldename des Benutzers definiert ist. Der Datensatz enthält allgemeine Informationen und UNIX-Benutzerinformationen. Es gibt einen Benutzer mit demselben Anmeldenamen in der Windows NT-Domäne, von der aus Sie Daten an das Benutzerprofil weitergeben. Tivoli SecureWay User Administration erkennt, dass diesen beiden Benutzerdatensätzen derselbe Anmeldename zugeordnet ist. Es erkennt außerdem, dass der Anmeldename **freddie** einem UNIX-Konto im Profil und einem Windows NT-Konto zugeordnet ist. Während des Weitergabevorgangs werden die Windows NT-Benutzerinformationen dem Benutzerdatensatz hinzugefügt, und die allgemeinen Benutzerinformationen werden im Benutzerdatensatz zusammengefügt.

Anmerkungen:

1. Wenn die Datenweitergabe aus einer verwalteten Ressource, die kein UNIX-System ist, erfolgt, verwendet der erstellte Datensatz den Anmeldenamen des Benutzers für das Konto als Kennwort. Wenn Sie vor der Verteilung des Profils an die Endpunkte kein Kennwort hinzufügen, wird das Kennwort für das Konto zum Anmeldenamen.
2. Die Datenweitergabe von einer UNIX-TMR stellt Kennwörter bereit, die anders als die Kennwörter von anderen Plattformen verarbeitet werden. Weitere Informationen zur Verarbeitung der Kennwörter während des Weitergabevorgangs finden Sie unter „Befehl 'wpasswd' verwenden" auf Seite 84.

Sie können UNIX-Benutzerkonten an ein Benutzerprofil, deren Basisverzeichnisse von einem nicht von TME verwalteten NFS-Server aus verfügbar sind. Zum Ändern dieser Basisverzeichnisse bzw. zum Erstellen neuer Basisverzeichnisse muss das Konto **root** auf dem TMR-Server allerdings über Schreibzugriff auf das NFS-Dateisystem verfügen.

Wenn Sie vorhandene Informationen an ein Benutzerprofil weitergeben, führt Tivoli SecureWay User Administration keine Standardwertegruppe für die Attribute der Benutzerdatensätze aus. Die Werte, die in den Systemdateien oder Datenbanken definiert sind, werden in die Benutzerdatensätze kopiert. Die Richtlinie für Gültigkeitsprüfung wird bei der Datenweitergabe ausgeführt, um vor dem Hinzufügen von Datensätzen im Profil sicherzustellen, dass alle Informationen der vorgegebenen Richtlinie entsprechen. Wenn Sie Standardwerte für gefüllte Benutzerdatensätze generieren möchten, verwenden Sie den Befehl **wgenusrdef**. Eine Beschreibung dieses Befehls finden Sie im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Mit dem Befehl **wpopusrs** können Sie Daten aus der in einer Datei angegebenen Liste mit Benutzern an ein Benutzerprofil weitergeben. Dadurch kann die Anzahl der für das Profil erstellten Benutzerdatensätze verringert werden. Wenn Sie aus einer Datei Daten an NetWare-Datensätze weitergeben, müssen in der Datei Anmeldenamen im Format *Anmeldename*.*Kontext*[.*Kontext* ...] definiert sein. Der Anmeldename muss im angegebenen Kontext definiert werden. Weitere Informationen finden Sie in der Beschreibung des Befehls **wpopusrs** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Bevor Sie an ein Benutzerprofil Daten aus einem NetWare-Endpunkt weitergeben, müssen Sie zunächst den Befehl **wsetnds** ausführen. Mit dem Befehl **wsetnds** wird das Konto gesetzt, das für die Anmeldung an der NDS-Baumstruktur verwendet wird, wenn Sie Daten an ein Benutzerprofil weitergeben oder auf der Basis des TME-Benutzers eine Verteilung ausführen. Darüber hinaus müssen Sie unter Umständen die Standardwertegruppen **nw_nds_context** und **nw_volume_restrictions** zurücksetzen. (Die Standardwertegruppe **nw_nds_context** wird auf der Tivoli-Arbeitsoberfläche als **NetWare-NDS-Kontext** angezeigt.)

Der Standardwert für die Standardwertegruppe **nw_nds_context** ist **CompanyName**. Wenn Sie diesen Namen durch eine aussagekräftigere Bezeichnung ersetzen, können Sie darüber hinaus eines der folgenden Suffixe an den Kontextnamen anhängen, um damit den Umfang der Datenweitergabe besser festzulegen. Wird kein Suffix angegeben, werden an das Benutzerprofil Daten aus dem angegebenen Kontext und dessen untergeordneten Kontexten weitergegeben.

. Es werden nur Daten aus dem angegebenen Kontext, nicht aber aus den untergeordneten Kontexten weitergegeben.

- Es werden Daten aus allen untergeordneten Kontexten, nicht aber aus dem angegebenen Kontext selbst weitergegeben.

Wird die Standardwertegruppe **nw_nds_context** geändert, so dass sie ein Suffix enthält, sollten Sie dieses Suffix vor der Erstellung neuer Benutzerdatensätze löschen. Andernfalls wird das Suffix dem Kontextnamen als Zeichenfolge angehängt, und der Kontextname wird dadurch ungültig. Als Folge davon ist der Benutzerkonto bei der Verteilung des Profils nicht im NDS-Kontext vorhanden.

Für die Standardwertegruppe **nw_volume_restrictions** ist kein Standardwert vorhanden. Sollen jedoch Daten für Benutzereinschränkungen weitergegeben werden, müssen Sie mindestens einen Datenträger im folgenden Format angeben:

*Datenträgername**.**Kontextname#Größe*

Beispiel:

```
SLOPPY_SYS.Tivolisys#
```

Dabei gilt Folgendes:

SLOPPY_SYS
Gibt den Datenträgernamen an.

Tivolisys
Gibt den Kontextnamen an.

Die Angabe des Nummernzeichens (#) ist erforderlich, die Angabe des Arguments *Größe* dagegeben optional. Dieses Argument gibt den Plattenspeicherplatz in KB an, der dem Benutzer auf dem angegebenen Datenträger zur Verfügung steht. Zulässig sind Werte zwischen 0 und 134.217.728 KB; die angegebene Zahl muss durch vier teilbar sein; ist dies nicht der Fall, wird die Angabe auf einen durch vier teilbaren Wert abgerundet. Bei Angabe von Null verfügt der Benutzer über keinen Schreibzugriff auf den Datenträger.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

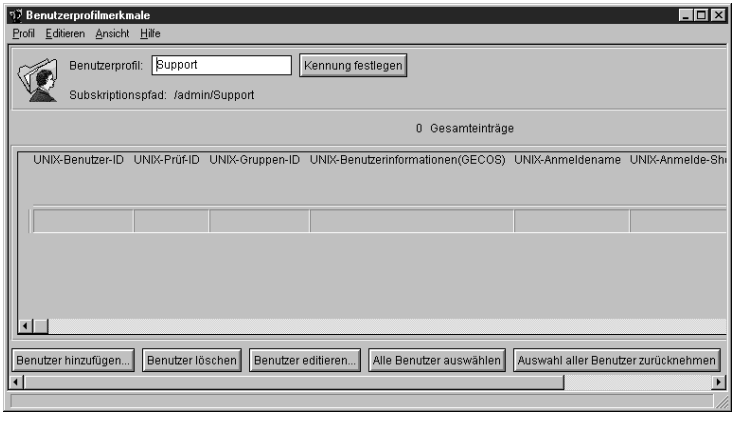
Aktivität	Umgebung	Berechtigungsklasse
Daten an Benutzerprofil weitergeben (Benutzerprofil ausfüllen)	Benutzerprofil	**admin**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Daten an ein Benutzerprofil weiterzugeben:

1. Klicken Sie in einem Profilmanager doppelt auf das Symbol eines Benutzerprofils, um das Fenster **Benutzerprofilmerkmale** anzuzeigen.



2. Wählen Sie **Ausfüllen** aus dem Menü **Profil** aus, um den Dialog **Profil ausfüllen** aufzurufen.

3. Wählen Sie in der Liste **Datensätze nicht aus folgenden Füllquellen abrufen** (früher: Datensätze nicht aus folgenden Weitergabequellen abrufen) die Tivoli-Ressourcen aus, von denen Daten an das Profil weitergegeben werden sollen. Wenn Sie Ressourcen auf unterschiedlichen Plattformarten auswählen, fügt Tivoli SecureWay User Administration die verschiedenen Standardsystemkonten nicht im Profil zusammen. Die Informationen von verschiedenen Plattformen für ein und denselben Anmeldenamen müssen mit dem Befehl **wpopusrs -m** zusammengefügt werden. Klicken Sie auf den Linkspfeil, um die ausgewählten Ressourcen in die Liste **Datensätze aus folgenden Füllquellen abrufen** (früher: Datensätze aus folgenden Weitergabequellen abrufen) zu verschieben.

   Weitere Informationen zu Standardsystemkonten finden Sie im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

4. Klicken Sie auf eines der folgenden Optionsfelder:

   - **An vorhandene Datensatzliste anfügen**

     Fügt die neuen Datensätze den vorhandenen Datensätzen im Profil hinzu. Verwenden Sie diese Option, wenn Sie Daten an ein Profil weitergeben, welches Datensätze enthält, die Sie beibehalten möchten.

   - **Vorhandene Datensatzliste überschreiben**

     Ersetzt die Benutzerdatensätze im Profil durch die neuen Datensätze.

     Anmerkung: Verwenden Sie diese Option mit Bedacht, da alle vorhandenen Datensätze im Profil verlorengehen. Werden Benutzerdatensätze bei einer Datenweitergabe gelöscht und nicht ersetzt, wird das betreffende Systemkonto bei der Verteilung des Profils gelöscht.

5. Klicken Sie auf **Ausfüllen und schließen**, um die Datensätze dem Profil hinzuzufügen und den Dialog zu schließen.

   Tivoli SecureWay User Administration fügt dem Profil die Konten aus den angegebenen Systemen hinzu.

Befehlszeile

Im folgenden Beispiel werden Daten an ein Benutzerprofil weitergegeben:

```
wpopusrs –o –l @ManagedNode:olympus @UserProfile:firestorm
```

Dabei gilt Folgendes:

–o Überschreibt den aktuellen Inhalt des Profils.

Anmerkung: Verwenden Sie diese Option mit Bedacht, da alle vorhandenen Datensätze im Profil verlorengehen. Werden Benutzerdatensätze bei einer Datenweitergabe gelöscht und nicht ersetzt, wird das betreffende Systemkonto bei der Verteilung des Profils gelöscht.

–l Gibt an, dass das vorhandene Basisverzeichnis unverändert bleibt, wenn Benutzerkonten durch Überschreiben gelöscht werden.

@ManagedNode:olympus
Gibt den Namen des Systems an, von dem Daten weitergegeben werden sollen.

@UserProfile:firestorm
Gibt den Namen des Profils an, an das Daten weitergegeben werden sollen.

Weitere Informationen hierzu finden Sie in der Beschreibung des Befehls **wpopusrs** im Handbuch *Tivoli SecureWay User Administration Reference Manual.*

Standardwerte für Verteilung festlegen

Sie können die Standardwerte steuern, die von einem Profil bei seiner Verteilung durch Tivoli SecureWay User Administration verwendet werden. Wenn Sie ein Profil aus einem Profilmanager verteilen, werden Ihnen keine Optionen dafür angeboten, wie die Verteilung ausgeführt werden soll. Stattdessen verwendet die Anwendung die Standardoptionen, die Sie mit dem Dialog **Standardwerte für Verteilung festlegen** definieren. Die Standardwerte legen fest, welche Optionsfelder standardmäßig ausgewählt sind, wenn Sie den Dialog **Profil verteilen** über das Kontextmenü des Benutzerprofils oder über die Option **Verteilen** im Fenster **Benutzerprofilmerkmale** aufrufen. Die Standardwerte werden für jedes Profil gesetzt. Die Standardoptionen jedes Profils können sich von denen anderer Profile unterscheiden.

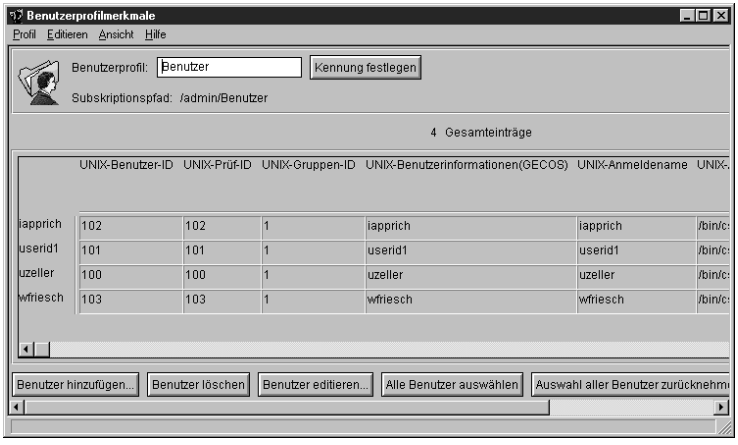
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Standardwerte für Verteilung festlegen	Profilmanager	**admin**

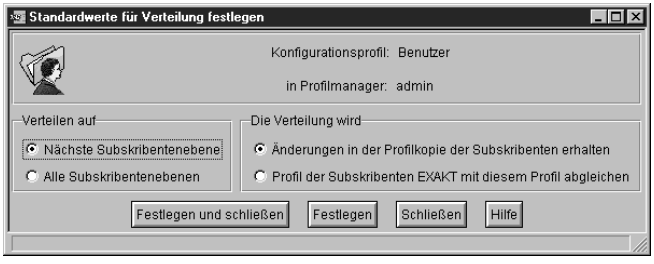
Sie können diese Task nur über die Tivoli-Arbeitsoberfläche ausführen.

Führen Sie folgende Schritte aus, um die Standardwerte eines Profils festzulegen:

1. Klicken Sie in einem Profilmanager doppelt auf das Symbol eines Benutzerprofils, um das Fenster **Benutzerprofilmerkmale** anzuzeigen.



2. Wählen Sie **Standardwerte verteilen** im Menü **Profil** aus, um den Dialog **Standardwerte für Verteilung festlegen** anzuzeigen.



3. Klicken Sie auf das Optionsfeld **Alle Subskribentenebenen**, um eine Kopie des Profils an die nächste Ebene von Subskribenten und deren Subskribenten zu senden. Verwenden Sie diese Option, wenn Sie alle Subskribenten auf der unteren Ebene in der Subskriptionshierarchie und sogar die eigentlichen Systemdateien der Profilendpunkte ändern möchten.

   — ODER —

   Klicken Sie auf **Nächste Subskribentenebene** im Feld **Verteilen auf**, um eine Kopie des Profils nur an die nächste Subskribentenebene zu senden. Verwenden Sie diese Option, wenn Sie die Kopien der Subskribenten auf der unteren Ebene in der Subskriptionshierarchie nicht ändern möchten.

Anmerkung: Wenn die nächste Ebene der Subskribenten die Ebene des verwalteten Knotens ist, wird das Profil nur an die Profilkopien auf dem verwalteten Knoten oder Endpunkt verteilt und nicht an die Systemdateien. Wenn Sie die Systemdateien mit Hilfe dieser Option ändern möchten, müssen Sie das Profil von der Ebene des verwalteten Knotens verteilen.

4. Klicken Sie auf **Änderungen in der Profilkopie der Subskribenten erhalten** im Feld **Die Verteilung wird**, um Änderungen beizubehalten, die Administratoren an den Profilen vorgenommen haben, deren Profilmanager dem aktuellen Profil zugeordnet sind. Verwenden Sie diese Option, wenn Profile in Subskribenten definiert wurden, deren Unterschiede Sie beibehalten möchten.

   — ODER —

   Klicken Sie auf das Optionsfeld **Profil der Subskribenten EXAKT mit diesem Profil abgleichen**, um die Änderungen, die Administratoren an ihren Profilen vorgenommen haben, mit den in diesem Profil definierten Werten zu überschreiben. Verwenden Sie diese Option, wenn Sie die Unterschiede zwischen den Profilen der Subskribenten nicht beibehalten möchten.

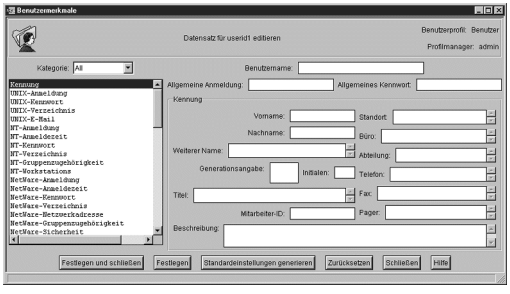
   Anmerkung: Wenn Sie dieses Optionsfeld verwenden, wird der gesamte Profilinhalt auf den Endpunkt geschrieben. *Alle vorgenommenen Änderungen, einschließlich der Kennwortänderungen durch den Benutzer, werden überschrieben.*

5. Klicken Sie auf **Festlegen und schließen**, um die Standardoptionen festzulegen und zum Dialog **Benutzerprofilmerkmale** zurückzukehren.

6

Benutzerdatensätze erstellen

In diesem Kapitel erfahren Sie, wie neue Benutzerdatensätze erstellt werden. Tivoli SecureWay User Administration speichert die neuen Benutzerinformationen in der Benutzerprofildatenbank und erstellt erst ein neues Systemkonto, wenn Sie das Profil an seine Subskribenten verteilen.



Es gibt drei voneinander abhängige Komponenten im Dialog **Benutzermerkmale**: die Dropdown-Liste **Kategorie**, die Merkmalliste (direkt darunter) und den Merkmalbereich (der Bereich unmittelbar rechts neben der Merkmalliste). Die aktuelle Auswahl in der Dropdown-Liste **Kategorie** legt fest, welche Optionen in der Merkmalliste angezeigt werden. Die aktuelle Auswahl in der Merkmalliste bestimmt die Anzeige im Merkmalbereich des Dialogs.

Wenn Sie beispielsweise die Option **Allgemein** in der Dropdown-Liste **Kategorie** und anschließend die Option **Subskribenten** in der Merkmalliste auswählen, zeigt Tivoli SecureWay User Administration im Merkmalbereich des Dialogs die Informationen zu den **Subskribenten** an.

Neue Datensätze für Benutzerkonten erstellen

Benutzerdatensätze enthalten sämtliche Informationen, die zum Verwalten der Benutzerkonten erforderlich sind. Bei der Erstellung eines neuen Benutzerdatensatzes wird dieser von Tivoli SecureWay User Administration in einer Datenbank für Benutzerprofile gespeichert. Die neuen Benutzerinformationen werden erst dann zu Systemdateien hinzugefügt, wenn Sie das Profil an seine endgültigen Endpunkte verteilen.

Wenn Sie einen neuen Benutzerdatensatz erstellen, können Sie Informationen für Windows NT-, Windows 2000-, NetWare- und UNIX-Benutzerkonten eingeben. Darüber hinaus können Sie allgemeine Benutzerinformationen eingeben.

In den Schritten, die unter „Standardwertegruppen definieren” auf Seite 132 beschrieben werden, erfahren Sie, wie die Standardwertegruppe für ein Profil festgelegt wird. Wenn Sie einen neuen Datensatz einem Profil hinzufügen, können Sie Informationen manuell hinzufügen und/oder Standardwertegruppen zum Eingeben von Informationen verwenden.

Wenn Sie im Dialog **Benutzermerkmale** auf **Standardeinstellungen generieren** oder **Hinzufügen** klicken, übernimmt Tivoli SecureWay User Administration die Standardwertegruppe, die für dieses Profil festgelegt wurde. Die Standardwertegruppe wird für ein Feld nicht übernommen, wenn Sie in diesem bereits Informationen eingegeben haben oder wenn Sie die Standardwertegruppe für dieses Attribut auf **Keine** gesetzt haben. Bei der Verwendung von Standardwertegruppen ist für die Erstellung eines Benutzerkontos nur eine Angabe im Feld **Benutzername** erforderlich.

Anmerkung: Beim Öffnen einer Dialoganzeige mit Kontrollkästchen bzw. Optionsfenstern werden die gesetzten Werte angezeigt. Daher wird die Standardwertegruppe nicht für diese Attribute übernommen.

Tivoli SecureWay User Administration wird mit einer Reihe von Standardwertegruppen geliefert. Zum Verwenden dieser Standardwertegruppen müssen Sie den Namen des Benutzers im Feld **Benutzername** eingeben (zum Beispiel Jon Smith) und anschließend auf **Standardeinstellungen generieren** klicken.

Mit den Standardwertegruppen werden den Windows NT-, Windows 2000-, NetWare- und UNIX-Konten für diesen Benutzerdatensatz Attributwerte zugeordnet und dem Benutzer die Steuerung der Kennwörter der einzelnen Konten ermöglicht; darüber hinaus werden der Anmeldename und das Kennwort des Benutzers für jedes Konto auf den ersten Buchstaben des Vornamens und den Nachnamen gesetzt (z. B. **jsmith**).

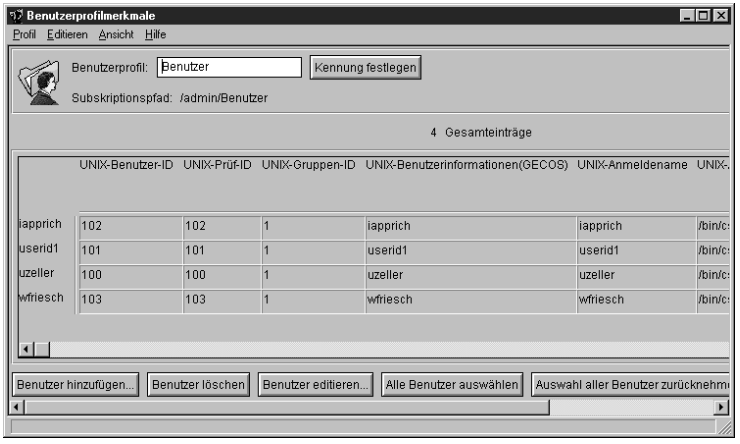
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklassen, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklassen
Datensatz für ein Benutzerkonto erstellen	Benutzerprofil	**admin** **Admin_Add_Account** **Admin_Edit_Account**

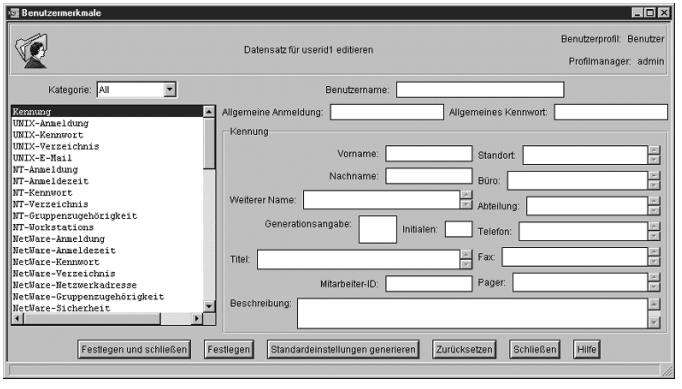
Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Führen Sie folgende Schritte aus, um einen Datensatz für ein Benutzerkonto zu erstellen:

1. Klicken Sie im Richtlinienbereich doppelt auf den entsprechenden Profilmanager, um das Fenster **Profilmanager** anzuzeigen.
2. Klicken Sie doppelt auf das Benutzerprofil, dem der neue Benutzer hinzugefügt werden soll. Das Fenster „Benutzerprofilmerkmale” wird angezeigt.



3. Klicken Sie auf **Benutzer hinzufügen**, um den Dialog **Benutzermerkmale** anzuzeigen.



4. Geben Sie den tatsächlichen Namen des Benutzers (Vor- und Nachname) im Feld **Benutzername** ein.

5. Geben Sie den aus einer Zeichenfolge bestehenden allgemeinen Anmeldenamen des Benutzers im Feld **Allgemeine Anmeldung** ein. Diesen Anmeldenamen kann dieser Benutzer als einzigen Anmeldenamen für jedes definierte Benutzerkonto verwenden.

   Ein Anmeldename kann alphanumerische Zeichen, Unterstriche (_), Gedankenstriche (-) und Punkte (.) sowie Leerzeichen ent-

halten. Außer diesen dürfen keine anderen Sonderzeichen verwendet werden, selbst wenn diese von dem jeweiligen Betriebssystem unterstützt werden.

6. Geben Sie das allgemeine Kennwort des Benutzers im Feld **Allgemeines Kennwort** ein. Dieses Kennwort kann der Benutzer als einziges erforderliches Kennwort für jedes definierte Benutzerkonto verwenden.
7. Klicken Sie auf **Standardeinstellungen generieren**, um Ihre definierten Standardwertegruppen für dieses Profil zu verwenden.

   Anmerkung: Sie können jederzeit auf **Standardeinstellungen generieren** klicken, um die Felder mit der für sie angegebenen Standardwertegruppe zu füllen.
8. Wählen Sie eine Option in der Dropdown-Liste **Kategorie** aus. Im Dialog **Benutzermerkmale** wird ein neuer Bereich angezeigt, in dem Sie Benutzerattribute setzen können.

   Anmerkung: Sie können eine Betriebssystemart in der Dropdown-Liste **Kategorie** auswählen, um die Anzahl der angezeigten Kategorien zu begrenzen.
9. Geben Sie die Benutzerinformationen für diesen Benutzer ein. Weitere Einzelheiten zum Eingeben von Benutzerinformationen für jede Betriebssystemart finden Sie in den folgenden Abschnitten:
   - Allgemeine Informationen zu Benutzerkonten
   - Informationen zu Windows NT-Benutzerkonten
   - Informationen zu Windows 2000-Benutzerkonten
   - Informationen zu NetWare-Benutzerkonten
   - Informationen zu UNIX-Benutzerkonten
10. Klicken Sie auf **Hinzufügen und schließen**, um diesen Benutzerdatensatz dem Benutzerprofil hinzuzufügen. Wenn Sie noch nicht auf **Standardeinstellungen generieren** geklickt haben, übernimmt Tivoli SecureWay User Administration in den Feldern, für die Standardwertegruppen definiert wurden und die noch leer sind, die entsprechenden Werte.

Allgemeine Informationen zu Benutzerkonten

Bestimmte Benutzerinformationen sind unabhängig vom verwendeten Betriebssystem. Folgendes gehört zu den allgemeinen Benutzerinformationen:

- Benutzer-ID
- Postadresse
- Informationen zu Subskribenten
- Informationen zur Sicherheitsgruppe
- Informationen zur Sicherheitsrichtlinie

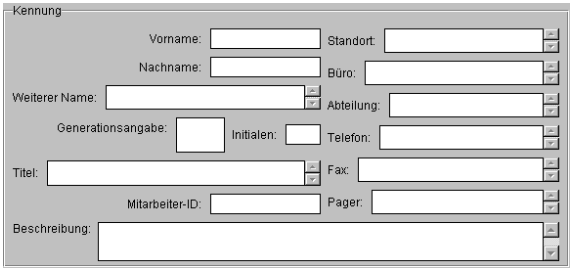
Führen Sie folgende Schritte aus, um allgemeine Informationen zu Benutzerkonten einzugeben:

1. Wählen Sie in der Dropdown-Liste **Kategorie** die Option **Allgemein** aus.
2. Wählen Sie die gewünschte Option in der Merkmalliste aus, und geben Sie die Benutzerinformationen ein.

Informationen zur Benutzeridentifikation

Mit der Option für die Benutzer-ID-Informationen können Sie allgemeine Informationen zum Benutzer wie zum Beispiel Namen, Rufnummer und die Berufsbezeichnung eingeben.

1. Wählen Sie in der Liste **Kategorie** die Option **Kennung** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



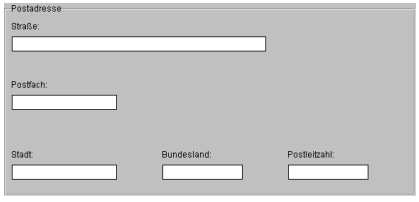
2. Geben Sie die Benutzerdaten wie gewünscht ein. Beachten Sie bei der Definition der Benutzerdaten Folgendes:
   - Alle Felder im Bereich **Kennung** sind optional.

- Jedes Feld kann mehr als 50 Zeichen enthalten.
- Jr., Sr. und II sind Beispiele für Generationsangaben.
- Das Feld **Titel** gibt die Berufsbezeichnung des Benutzers an.

Informationen zur Postadresse

Mit der Option für Informationen zur Postadresse können Sie die Postadresse des Benutzers eingeben.

1. Wählen Sie **Postadresse** in der Merkmalliste aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Geben Sie die Informationen zur Postadresse des Benutzers ein.

Informationen zu Subskribenten

Mit der Subskribentenoption können Sie die Endpunkte auswählen, denen ein Benutzerdatensatz zugeordnet wird. Bei diesen Subskribenten kann es sich um Windows NT-Domänenserver, Windows 2000-Serverendpunkte, Novell NetWare-NDS-Serverendpunkte, UNIX-verwaltete Knoten und Endpunkte, NIS-Domänen und andere verwaltete Knoten bzw. andere Profilmanager handeln. Bei der Verteilung eines Profils sendet Tivoli SecureWay User Administration dieses an jeden Profilendpunkt. Anschließend legt die Anwendung auf Datensatzebene fest, welche Datensätze den jeweiligen Profilendpunkten zugeordnet werden. Diese Option bietet Ihnen mehr Flexibilität, wenn Sie ein Profil verteilen. Weitere Informationen finden Sie unter „Profile verteilen” auf Seite 26.

Diese Einrichtung für Subskriptionen auf Datensatzebene in Tivoli SecureWay User Administration basiert auf den Management Framework-Einrichtungen für die Profilmanagersubskription und die Profilverteilung. Die grundsätzliche Funktionsweise dieser Management Framework-Einrichtungen wird von Subskriptionen auf Datensatzebene nicht beeinflusst. Bei der Verteilung eines Profils an alle Ebe-

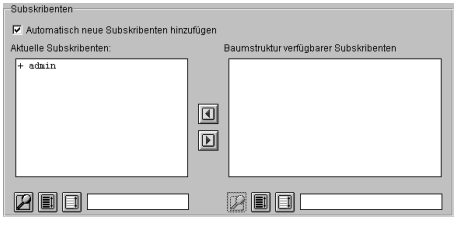
nen wird dieses daher an jeden Subskribenten gesendet, der dem Profilmanager dieses Profils zugeordnet ist. Bei Eingang des Profils auf einem Profilendpunkt, entscheidet Tivoli SecureWay User Administration anhand der Subskriptionsdaten des Benutzers auf Datensatzebene, ob die Benutzerinformationen auf dem betreffenden Endpunkt aktualisiert werden sollen oder nicht.

AEF-Endpunktvorgänge werden unabhängig von den Subskriptionsdaten eines Benutzers auf Datensatzebene ausgeführt. Diese Aktionsskripts sollten die Subskriptionsdaten auf Datensatzebene überprüfen, um die Notwendigkeit einer Ausführung festzustellen. Weitere Informationen zu AEF-Endpunktvorgängen finden Sie im Handbuch *Tivoli AEF User's Guide*.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Subskribenteninformationen einzugeben:

1. Wählen Sie **Subskribenten** in der Merkmalliste aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



Standardmäßig wird in der Liste **Aktuelle Subskribenten** der Profilmanager angezeigt, der das Benutzerprofil enthält, mit dem Sie arbeiten. Daraus geht hervor, dass der Profilmanager und alle Endpunkte, die dem Profilmanager zugeordnet sind, auch dem Benutzerdatensatz zugeordnet sind. Ein Pluszeichen (+) gibt an, dass die Liste mit Subskribenten erweitert werden kann, ein Minuszeichen (-), dass die Verzweigung einer Subskribentenhierarchie bzw. -baumstruktur bereits erweitert wurde.

2. Wenn die Liste der angezeigten Subskribenten geändert werden soll, müssen Sie den Profilmanager in die Liste **Baumstruktur verfügbarer Subskribenten** verschieben und die Baumstruktur erweitern. Führen Sie folgende Schritte aus, um Subskribenteninformationen zu ändern:

   a. Wählen Sie in der Liste **Aktuelle Subskribenten** eine Option aus, und klicken Sie auf den Rechtspfeil. Die ausgewählte Option wird daraufhin in die Liste **Baumstruktur verfügbarer Subskribenten** verschoben.

      Anmerkung: Einträge können nicht durch Doppelklicken in eine andere Liste verschoben werden.

   b. Sollen Einträge mit einem Pluszeichen (+) erweitert werden, klicken Sie doppelt auf die betreffende Option. Die Liste wird daraufhin aktualisiert, und es werden alle der Option direkt zugeordneten Subskribenten angezeigt. Wiederholen Sie diesen Schritt, so oft es erforderlich ist.

   c. Wählen Sie eine Option aus, der in die Liste **Aktuelle Subskribenten** verschoben werden soll. Klicken Sie anschließend auf den Linkspfeil. Die ausgewählte Option wird daraufhin in die Liste **Aktuelle Subskribenten** verschoben.

3. Klicken Sie auf das Kontrollkästchen **Automatisch neue Subskribenten hinzufügen**, um automatisch alle Änderungen an den Subskribenten des Profilmanagers zu übernehmen, nachdem die Subskriptionen auf Datensatzebene gesetzt wurden. Nach jeder Änderung an den Subskribenten des Profilmanagers werden diese Änderungen auf Datensatzebene übernommen.

   Anmerkung: Da ein Profilendpunkt (bzw. ein Profilmanager) an mehreren Stellen innerhalb der Subskribentenstruktur angezeigt werden kann, kann der Name dieses Profilendpunkts ebenfalls mehrmals in der Liste **Aktuelle Subskribenten** vorkommen. Diese Duplikate werden vor dem Schreiben des Benutzerdatensatzes entfernt.

Befehlszeile

Die Argumente **-su** und **-ns** des Befehls **wcrtusr** entsprechen den Feldern **Aktuelle Subskribenten** und **Automatisch neue Subskribenten hinzufügen** auf der Tivoli-Arbeitsoberfläche. Standardmäßig wird der Datensatz bei Angabe des Arguments **-su** an alle Subskribenten in der Subskriptionshierarchie verteilt und das Argument **-ns** auf **ENABLED** gesetzt. Diese Standardwerte werden nicht durch die Standardwertegruppe festgelegt. Daher können die Standardwerte auch nicht geändert werden. Mit der gemeinsamen Angabe der Argumente **-su** und **-ns** werden die Attribute **subscribers** und **add_new-_subscribers** gesetzt. Diese Attribute können zum Festlegen der Richtlinie für Gültigkeitsprüfung und in anderen Skriptarten verwendet werden.

Für das Argument **-su** kann eine Liste mit Profilendpunkten (jeweils durch ein Komma voneinander getrennt) angegeben werden, die dem Datensatz zugeordnet sind. An Stelle einer solchen Liste können Sie auch eines der folgenden Sonderzeichen angeben:

***** Gibt an, dass der Benutzerdatensatz allen Mitgliedern der Subskriptionsbaumstruktur zugeordnet wird. Die Angabe dieses Sonderzeichens entspricht der Angabe des Profilmanagers der höchsten Ebene.

\# Gibt an, dass der Benutzerdatensatz keinen Subskribenten zugeordnet ist.

Wird das Argument **-ns** auf **ENABLED** gesetzt, enthält das Attribut **subscribers** die Namen der Endpunkte, die *nicht* mit dem Argument **-su** aufgeführt wurden. Tivoli SecureWay User Administration kann nicht zwischen Endpunkten unterscheiden, die bei der Ausführung des Befehls **wcrtusr** absichtlich nicht angegeben wurden, und Endpunkten, die im Nachhinein der TMR hinzugefügt wurden. Im Folgenden werden die möglichen Werte des Attributs **subscribers** erläutert.

In der folgenden Tabelle sind die möglichen Werte der Argumente **-su** und **-ns** sowie deren Auswirkung auf das Attribut **subscribers** aufgeführt. In diesen Beispielen sind **ep1**, **ep2** und **ep3** auswählbare Ziele für eine Verteilung.

Wert für -ns	Wert für -su	Wert des Attributs 'subscribers'
ENABLED	*	Null
ENABLED	#	**ep1**, **ep2**, **ep3**
ENABLED	**ep1**, **ep2**	**ep3**
DISABLED	*	**ep1**, **ep2**, **ep3**
DISABLED	#	Null
DISABLED	**ep1**, **ep2**	**ep1**, **ep2**

Das Attribut **subscribers** enthielt ursprünglich lediglich eine sortierte Liste mit den Namen von Endpunkten. Jetzt enthält es andere Werte, die von allen Skripts, die den Inhalt dieses Attributs prüfen, ignoriert werden sollten. Diese Werte beginnen alle mit dem Nummernzeichen (#), das für Ressourcennamen in einer TMR nicht verwendet werden darf.

Weitere Informationen zum Hinzufügen und Bearbeiten von Benutzerdatensätzen über die Befehlszeile finden Sie in der Beschreibung des Befehls **wcrtusr** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

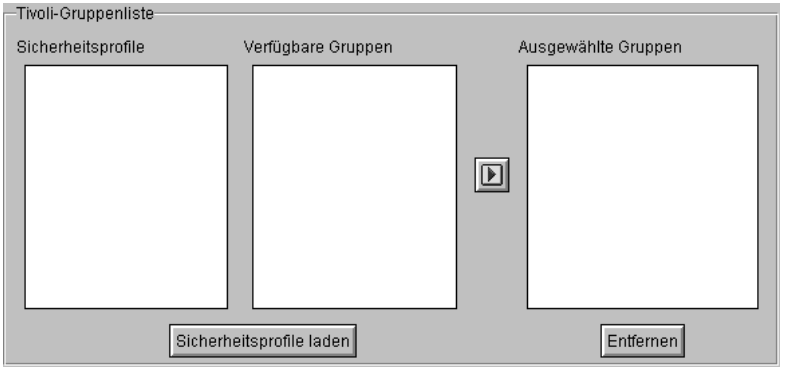
Informationen zur Sicherheitsgruppe

Mit der Option für **TME-Sicherheitsgruppen** können Sie einem Benutzerdatensatz Sicherheitsgruppenzugehörigkeiten von Tivoli SecureWay Security Manager zuordnen. Jeder Benutzerdatensatz kann mehrere Sicherheitsgruppenzugehörigkeiten besitzen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um einem Benutzerdatensatz Sicherheitsgruppenzugehörigkeiten von Tivoli SecureWay Security Manager zuzuordnen.

1. Wählen Sie die Option **TME-Sicherheitsgruppen** in der Merkmalliste aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Klicken Sie auf die Schaltfläche **Sicherheitsprofile laden**. Daraufhin wird nach allen verfügbaren Sicherheitsprofilen gesucht. Die verfügbaren Sicherheitsprofile werden dann in der Liste**Sicherheitsprofile** aufgeführt.
3. Wählen Sie ein Sicherheitsprofil in der Liste **Sicherheitsprofile** aus, um in der Liste **Verfügbare Gruppen** alle Sicherheitsgruppen anzuzeigen, die dem Profil zugeordnet sind.
4. Wählen Sie eine oder mehrere Sicherheitsgruppe(n) in der Liste **Verfügbare Gruppen** aus, und klicken Sie auf den Rechtspfeil. Dadurch werden die ausgewählten Gruppen in die Liste **Ausgewählte Gruppen** verschoben. Dieser Benutzerdatensatz wird allen Sicherheitsgruppenlisten in der Liste **Ausgewählte Gruppen** zugeordnet.

Anmerkungen:

1. Zum Hinzufügen von Sicherheitsgruppen aus anderen Sicherheitsprofilen wiederholen Sie die Schritte 3 und 4. Sicherheitsgruppen, die bereits in der Liste **Ausgewählte Gruppen** aufgelistet sind, verbleiben dort.
2. Wählen Sie zum Entfernen einer oder mehrerer Sicherheitsgruppen aus der Liste **Ausgewählte Gruppen** die Gruppen aus, und klicken Sie auf **Entfernen**.

Befehlszeile

Im folgenden Beispiel wird ein neuer Benutzerdatensatz hinzugefügt, der UNIX- und Windows NT-Benutzerinformationen enthält.

```
wcrtusr –e 5359 –dp Marketing –N –fn jon –ln smith –E –f \
olympus:/usr/template –H rushmore -h /users/jsmith \
–S olympus:/Noon/marketing/jsmith –L \
ENABLED –l jsmith –P jsmith –s /bin/csh –t MOUNTED –w \
ENABLED –At USER –ct ENABLED –Et ENABLED -Ft \
F:\PUBLIC\LOGIN –ht C: –Lt ENABLED –Pt Marketing \
@UserProfile:Marketing "Jon Smith"
```

Dabei gilt Folgendes:

–e 5359
Gibt die Rufnummer des Benutzers an.

–dp Marketing
Gibt die Abteilung an, zu der der Benutzer gehört.

–N Ermöglicht den Subskribenten, die Kopien des Benutzerkontodatensatzes zu ändern.

–fn jon
Gibt den Vornamen des Benutzers an.

–ln smith
Gibt den Nachnamen des Benutzers an.

–f olympus:/usr/template
Gibt die Speicherposition des ursprünglichen Inhalts im UNIX-Basisverzeichnis an.

–H rushmore
Gibt den Namen des UNIX-Mailservers des Benutzers an.

–h /users/jsmith
Gibt den Pfad für das lokale Basisverzeichnis an

–S olympus:/Noon/marketing/jsmith
Gibt die ferne Position des UNIX-Basisverzeichnisses des Benutzers auf dem NFS-Server ’Olympus’ an.

–L ENABLED
Aktiviert die UNIX-Anmeldung für diesen Benutzer.

–l jsmith
Gibt den UNIX-Anmeldenamen des Benutzers an.

–P jsmith
Gibt den E-Mail-Aliasnamen des Benutzers für UNIX an.

–s /bin/csh
Gibt die UNIX-Anmelde-Shell des Benutzers an.

–t MOUNTED
Gibt an, dass das UNIX-Basisverzeichnis entfernt angehängt ist.

–w ENABLED
Legt fest, dass das UNIX-Kennwort des Benutzers nur für die Erstanmeldung gültig ist.

–At USER
Gibt an, dass der Benutzer unter Windows NT die Kontoart USER besitzt.

–ct ENABLED
Ermöglicht, dass der Benutzer das Windows NT-Kennwort steuert.

–Et ENABLED
Legt fest, dass das Windows NT-Kennwort des Benutzers nur für die Erstanmeldung gültig ist.

–Ft F:\PUBLIC\LOGIN
Gibt den Pfad des Windows NT-Anmeldeskripts des Benutzers an.

–ht C:
Gibt die Position des Windows NT-Basisverzeichnisses an.

–Lt ENABLED
Aktiviert die Windows NT-Anmeldung des Benutzers.

–Pt Marketing
Gibt den Namen des Windows NT-Benutzerprofils an, dem dieser Benutzer hinzugefügt werden soll.

@UserProfile:Marketing
Gibt den Namen des Benutzerprofils an, dem dieser Benutzer hinzugefügt werden soll.

“Jon Smith”
Gibt den tatsächlichen Namen dieses Benutzers an.

Weitere Informationen zum Hinzufügen eines Benutzerdatensatzes zu einem Profil über die Befehlszeile finden Sie in der Beschreibung des Befehls **wcrtusr** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

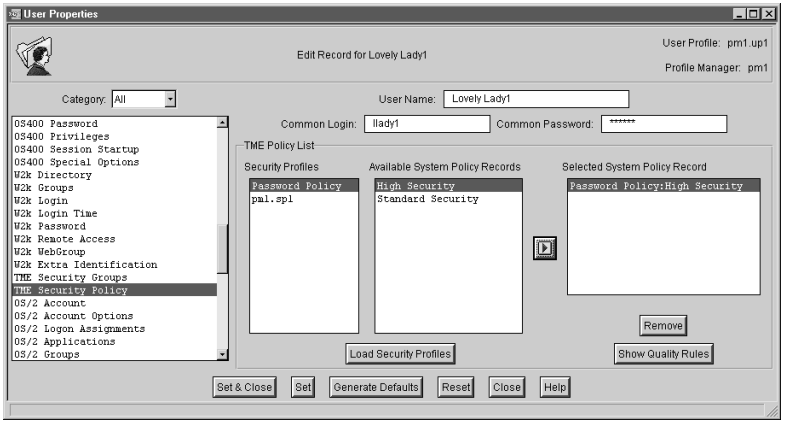
Informationen zur Sicherheitsrichtlinie

Über die Option **TME-Sicherheitsrichtlinie** kann ein Tivoli-Administrator einem bestimmten Benutzerdatensatz einen Systemrichtliniendatensatz in einem Sicherheitsprofil zuordnen. Außerdem werden dem Administrator auf der Tivoli-Arbeitsoberfläche die im ausgewählten Systemrichtliniendatensatz gespeicherten Qualitätsregeln für das Kennwort angezeigt.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um einem bestimmten Benutzerdatensatz einen Systemrichtliniendatensatz in einem Sicherheitsprofil zuzuordnen und die Qualitätsregeln in dem ausgewählten Systemrichtliniendatensatz anzuzeigen.

1. Wählen Sie die Option **TME-Sicherheitsrichtlinie** in der Merkmalliste aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** (User Properties) anzuzeigen:

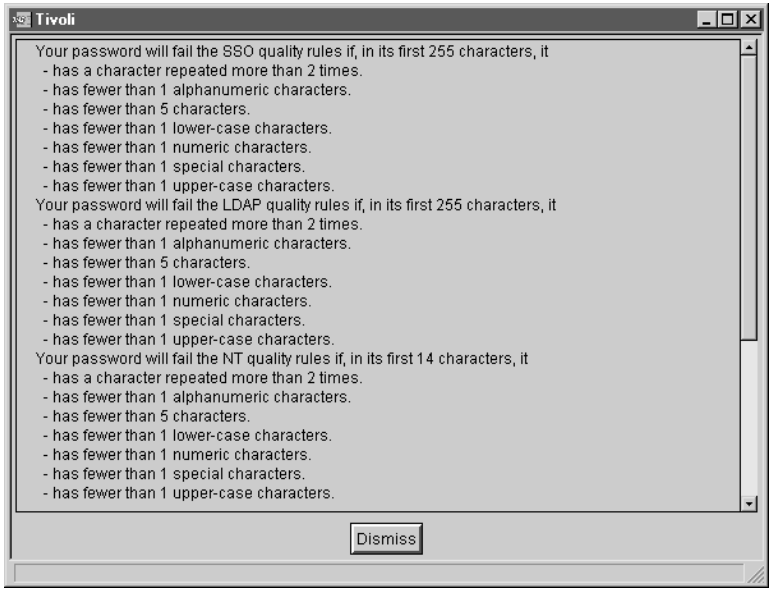


2. Klicken Sie auf die Schaltfläche **Sicherheitsprofile laden** (Load Security Profiles). Daraufhin wird nach allen verfügbaren Sicherheitsprofilen gesucht. Die verfügbaren Sicherheitsprofile werden dann in der Liste**Sicherheitsprofile** aufgeführt.

3. Wählen Sie ein Sicherheitsprofil in der Liste **Sicherheitsprofile** aus, um in der Liste **Verfügbare Gruppen** alle Sicherheitsrichtliniendatensätze anzuzeigen, die dem Profil zugeordnet sind.

4. Wählen Sie eine oder mehrere Sicherheitsrichtliniengruppe(n) in der Liste **Verfügbare Systemrichtliniendatensätze** (Available System Policy Records) aus, und klicken Sie auf den Rechtspfeil. Dadurch werden die ausgewählten Gruppen in die Liste **Ausgewählte Systemrichtliniendatensätze** (Selected System Policy Record) verschoben. Dieser Benutzerdatensatz wird allen Sicherheitsrichtliniendatensätzen in der Liste **Ausgewählte Systemrichtliniendatensätze** zugeordnet.

5. Wenn Sie die Qualitätsregeln wie im folgenden Beispiel anzeigen möchten, wählen Sie den gewünschten Systemrichtliniendatensatz in der Liste **Ausgewählte Systemrichtliniendatensätze** aus, und klicken Sie auf die Schaltfläche **Qualitätsregeln anzeigen** (Show Quality Rules).


Tivoli
Your password will fail the SSO quality rules if, in its first 255 characters, it
- has a character repeated more than 2 times.
- has fewer than 1 alphanumeric characters.
- has fewer than 5 characters.
- has fewer than 1 lower-case characters.
- has fewer than 1 numeric characters.
- has fewer than 1 special characters.
- has fewer than 1 upper-case characters.
Your password will fail the LDAP quality rules if, in its first 255 characters, it
- has a character repeated more than 2 times.
- has fewer than 1 alphanumeric characters.
- has fewer than 5 characters.
- has fewer than 1 lower-case characters.
- has fewer than 1 numeric characters.
- has fewer than 1 special characters.
- has fewer than 1 upper-case characters.
Your password will fail the NT quality rules if, in its first 14 characters, it
- has a character repeated more than 2 times.
- has fewer than 1 alphanumeric characters.
- has fewer than 5 characters.
- has fewer than 1 lower-case characters.
- has fewer than 1 numeric characters.
- has fewer than 1 special characters.
- has fewer than 1 upper-case characters.
Dismiss

Anmerkungen:

1. Wiederholen Sie zum Hinzufügen von Sicherheitsrichtliniendatensätzen aus anderen Sicherheitsprofilen die Schritte 3 und 4. Sicherheitsrichtliniendatensätze, die bereits in der Liste **Ausgewählte Systemrichtliniendatensätze** aufgelistet sind, verbleiben dort.
2. Wählen Sie zum Entfernen einer oder mehrerer Sicherheitsgruppen aus der Liste **Ausgewählte Systemrichtliniendatensätze** die zu entfernenden Systemrichtliniendatensätze aus, und klicken Sie auf **Entfernen** (Remove).

Befehlszeile

Im folgenden Beispiel wird ein neuer Benutzerdatensatz hinzugefügt, dem ein ausgewählter Sicherheitsprofildatensatz in einem bestimmten Sicherheitsprofil zugeordnet ist:

```
wcrtusr -sp @SecurityProfile:pml.sp1:Kennwortqualität
```

Dabei gilt Folgendes:

–sp @SecurityProfile:pml.sp1
: Gibt **pml.sp1** als Namen des Sicherheitsprofils an, in dem der gewünschte Systemrichtliniendatensatz enthalten ist (entweder mit oder ohne Initiale **@SecurityProfile:**)

Kennwortqualität
: Gibt den Kennsatz des Systemrichtliniendatensatzes an.

Weitere Informationen zum Hinzufügen eines Benutzerdatensatzes und zum Zuordnen zu einem ausgewählten Systemrichtliniendatensatz in einem Sicherheitsprofil über die Befehlszeile finden Sie in der Beschreibung der Befehle **wcrtusr –sp**, **wgetusr –sp** oder **wsetusr –sp** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Informationen zu Windows NT-Benutzerkonten

Mit Tivoli SecureWay User Administration können Sie Benutzerkonten für Windows NT verwalten. Folgende Informationen können Sie für einen Windows NT-Benutzerdatensatz eingeben:

- Anmeldeinformationen
- Anmeldezeiten
- Kennwortinformationen
- Informationen zum Basisverzeichnis
- Informationen zur Gruppenzugehörigkeit
- Informationen zu Workstations
- Informationen zum Fernzugriff

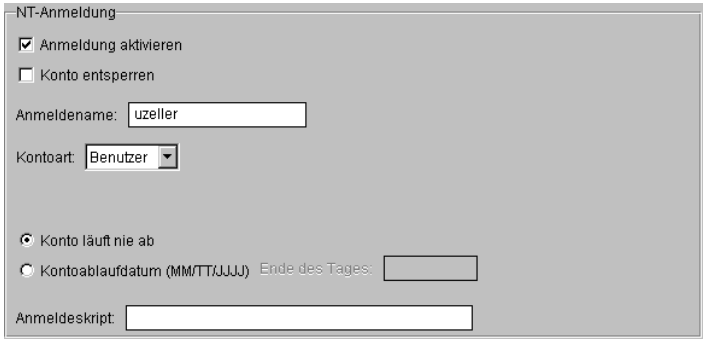
Führen Sie folgende Schritte aus, um Benutzerinformationen für Windows NT hinzuzufügen:

1. Wählen Sie in der Dropdown-Liste **Kategorie** die Option **NT** aus.
2. Wählen Sie die gewünschte Option in der Merkmalliste aus.

Informationen zur Windows NT-Anmeldung

Mit der Option für Windows NT-Anmeldungen können Sie die Anmeldeinformationen für Windows NT eingeben.

1. Wählen Sie **NT-Anmeldung** in der Merkmalliste aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Wählen Sie das Kontrollkästchen **Anmeldung aktivieren** aus, um die Anmeldung dieses Benutzers zu aktivieren.
3. Geben Sie im Feld **Anmeldename** den Anmeldenamen des Benutzers ein. Der Anmeldename kann 1 bis 20 alphanumerische Zeichen (einschließlich Leerzeichen) enthalten.
4. Wählen Sie die entsprechende Kontoart in der Dropdown-Liste **Kontoart** aus. Die folgenden Optionen sind verfügbar:

   Keine Gibt eine ungültige Kontoart an.

   Admin
   Fügt diesen Benutzer der Gruppe der Domänenadministratoren hinzu.

   Benutzer
   Fügt diesen Benutzer der Gruppe der Domänenbenutzer hinzu.

   Gast Fügt diesen Benutzer der Gruppe der Domänengäste hinzu.

5. Klicken Sie auf eines der folgenden Optionsfelder:

   Konto läuft nie ab
   Bei Auswahl dieser Option bleibt das Konto für eine unbestimmte Zeit aktiv.

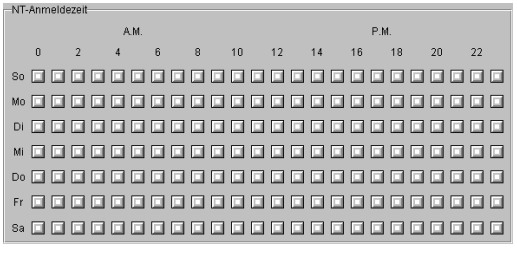
   Kontoablaufdatum
   Mit dieser Option wird das Ablaufdatum für das Konto festgelegt. Das Datum muss im Format *MM*/*TT*/*JJJJ* eingegeben werden. Ab dem angegebenen Datum ist das Konto nicht länger gültig.

6. Geben Sie im Feld **Anmeldeskript** den Pfad für das Anmeldeskript des Benutzers ein.

Informationen zur Windows NT-Anmeldezeit

Mit der Option **Anmeldezeit** können Sie die Uhrzeiten festlegen, zu denen sich der betreffende Benutzer unter diesem Benutzerkonto am Netzwerk anmelden kann.

1. Wählen Sie in der Merkmalliste die Option **NT-Anmeldezeit** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:

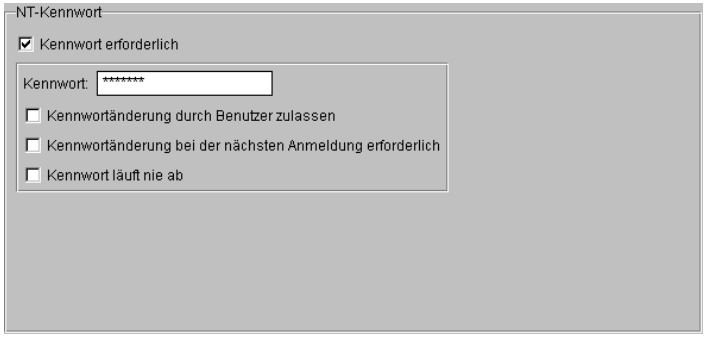


2. Wählen Sie die Uhrzeiten und Tage aus, auf die Sie den Zugriff des Benutzers auf das Netzwerk beschränken möchten, indem Sie die entsprechenden Kontrollkästchen auswählen. Ein ausgewähltes Kontrollkästchen wird dunkel dargestellt (der weiße Punkt ist nicht sichtbar). Wenn Sie keine Kontrollkästchen auswählen, kann sich der Benutzer jederzeit anmelden.

Informationen zum Windows NT-Kennwort

Mit der Option **NT-Kennwort** können Sie das Kennwort des Benutzers festlegen und bestimmte Optionen für dieses Kennwort auswählen.

1. Wählen Sie in der Merkmalliste die Option **NT-Kennwort** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:

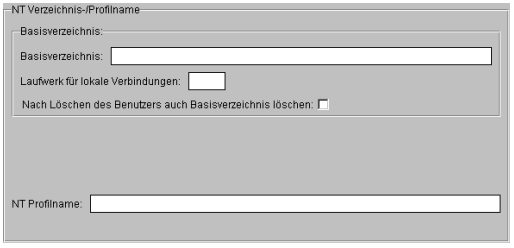


2. Geben Sie im Feld **Kennwort** das Kennwort des Benutzers ein.
3. Wählen Sie das Kontrollkästchen **Kennwort erforderlich** aus, wenn für dieses Benutzerkonto ein Kennwort erforderlich ist.
4. Wählen Sie das Kontrollkästchen **Kennwortänderung durch Benutzer zulassen** aus, wenn der Benutzer die Möglichkeit erhalten soll, das Kennwort zu ändern. Andernfalls kann das Kennwort nur vom Administrator geändert werden.
5. Wählen Sie das Kontrollkästchen **Kennwortänderung bei der nächsten Anmeldung erforderlich** aus, wenn der Benutzer das Kennwort bei der nächsten Anmeldung nach der Verteilung des Profils ändern soll.
6. Wählen Sie das Kontrollkästchen **Kennwort läuft nie ab** aus, wenn für den Benutzer keine Notwendigkeit einer Kennwortänderung bestehen soll.

Informationen zum Windows NT-Verzeichnis

Mit der Option **NT-Verzeichnis** können Sie das Basisverzeichnis erstellen und definieren.

1. Wählen Sie in der Merkmalliste die Option **NT-Verzeichnis** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Geben Sie im Feld **Basisverzeichnis** den Pfad für das Basisverzeichnis des Benutzers ein. Der angegebene Wert kann lokal oder fern sein. Beispiel für ein Verzeichnis im lokalen Dateisystem: **C:\Basisverzeichnis**. Beispiel für ein Verzeichnis in einem fernen Dateisystem: **\\Server\Users\Basisverzeichnis**.
3. Geben Sie im Feld **Laufwerk für lokale Verbindungen** das Laufwerk ein, an das die fernen Verzeichnisse bei der Anmeldung des Benutzers angehängt werden. Die Angabe eines Doppelpunktes nach dem Laufwerkbuchstaben ist optional.
4. Wählen Sie das Kontrollkästchen **Nach Löschen des Benutzers auch Basisverzeichnis löschen** aus, wenn das Basisverzeichnis beim Löschen des Benutzerdatensatzes aus dem Benutzerprofil ebenfalls gelöscht werden soll. Das Verzeichnis wird in diesem Fall erst bei der Verteilung des Profils gelöscht.
5. Geben Sie im Feld **NT-Profilname** den Pfad für das Windows NT-Benutzerprofil ein. Über ein Windows NT-Benutzerprofil wird die Umgebung festgelegt, die vom System bei der Anmeldung des Benutzers geladen wird. Der Pfad muss im Format *Servername**Profilordnername**Profilname* eingegeben werden.

Informationen zur Windows NT-Gruppenzugehörigkeit

Mit der Option **NT-Gruppenzugehörigkeit** können Sie die Windows NT-Gruppenzugehörigkeit für diesen Benutzer definieren.

1. Wählen Sie in der Merkmalliste die Option **NT-Gruppenzugehörigkeit** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:

2. Geben Sie den Namen der Gruppe ein, zu der dieser Benutzer gehört, und klicken Sie auf **Hinzufügen**. Die Gruppe wird daraufhin der entsprechenden Liste hinzugefügt. Wiederholen Sie diesen Schritt, so oft es erforderlich ist.

Informationen zu Windows NT-Workstations

Mit der Option NT-Workstations können Sie festlegen, von welchen Windows NT-Workstations aus sich der Benutzer mit diesem Benutzerkonto am Netzwerk anmelden kann.

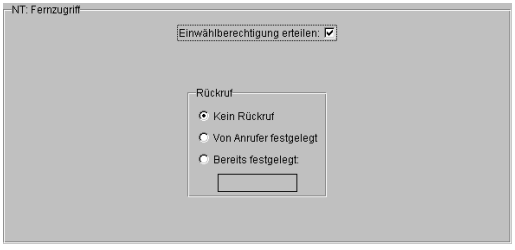
1. Wählen Sie in der Merkmalliste die Option **NT-Workstations** aus.

2. Geben Sie die Workstation ein, von der sich dieser Benutzer am Netzwerk anmelden kann, und klicken Sie auf **Hinzufügen**. Der Name der Workstation wird daraufhin der entsprechenden Liste hinzugefügt. Wiederholen Sie diesen Schritt, so oft es erforderlich ist.

Informationen zum Windows NT-Fernzugriff

Mit der Option **NT-Fernzugriff** können Sie die Einwählberechtigungen für einen Benutzer festlegen. Diese Berechtigungen gelten nur für RAS-Server (Remote Access Service).

1. Wählen Sie in der Merkmalliste die Option **NT-Fernzugriff** aus.



2. Wählen Sie das Kontrollkästchen **Einwählberechtigung erteilen** aus, um dem Benutzer den RAS-Zugriff zu ermöglichen und den Bereich **Rückruf** zu aktivieren.

3. Bei Aktivierung der Windows NT-RAS-Rückrufoption stellt der Benutzer über einen Anruf eine Verbindung zum RAS-Server her. Der RAS-Server trennt die Verbindung und ruft unmittelbar danach die vorgegebene bzw. die vom Benutzer angegebene Rufnummer zurück. Klicken Sie auf eines der folgenden Optionsfelder, um die Rückrufoption für den Benutzer festzulegen:

   Kein Rückruf

   Die Rückruffunktion ist nicht aktiviert. Der Benutzer kann sich einwählen und erhält unmittelbaren Zugriff auf das System.

Von Anrufer festgelegt

Die vom Benutzer angegebene Rufnummer wird zurückgerufen. Diese Funktion ist ausgesprochen hilfreich für Benutzer, die sich von verschiedenen Standorten aus und unter verschiedenen Rufnummern einwählen.

Bereits festgelegt

Die angegebene Rufnummer wird zurückgerufen. Diese Option sollte für ferne Computer an festen Standorten, wie beispielsweise das Büro zu Hause, angegeben werden.

Anmerkung: Wird **Kein Rückruf** oder **Von Anrufer festgelegt** aktiviert und ist gleichzeitig im Feld **Bereits festgelegt** noch eine Rufnummer angegeben, kommt es unter Umständen zu Konflikten zwischen den Einträgen im Tivoli-Benutzerprofil und in der RAS-Datenbank auf dem Windows NT-Server. Dies führt unter Umständen dazu, dass Sie über den NT-Benutzer-Manager keine neue Rufnummer eingeben können. Dieses Problem kann umgangen werden, indem Sie über die Richtlinie für Gültigkeitsprüfung die Eingabe einer Rufnummer durch den Administrator bzw. das System verhindern, wenn das Kontrollkästchen **Bereits festgelegt** nicht aktiviert ist.

Informationen zu Windows 2000-Benutzerkonten

Mit Tivoli SecureWay User Administration können Sie Benutzerkonten für Windows 2000 verwalten. Folgende Informationen können Sie für einen Windows 2000-Benutzerdatensatz eingeben:

- Verzeichnis
- Gruppen
- Anmeldung
- Anmeldezeit
- Kennwort
- Fernzugriff
- Webgruppe
- Zusätzliche Identifikation

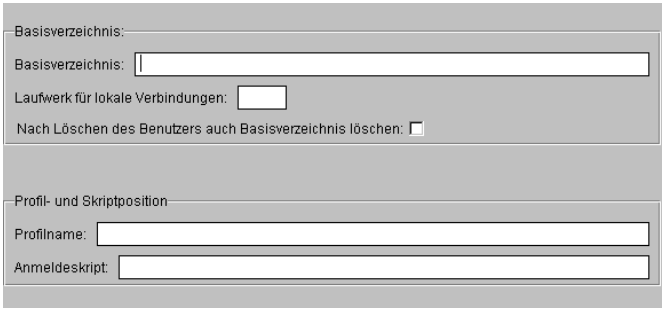
Führen Sie folgende Schritte aus, um Benutzerinformationen für Windows 2000 hinzuzufügen:

1. Wählen Sie in der Dropdown-Liste **Kategorie** die Option **Windows 2000** aus.
2. Wählen Sie die gewünschte Option in der Merkmalliste aus.

Windows 2000-Verzeichnis

Mit der Option **Windows 2000-Verzeichnis** können Sie Verzeichnisinformationen für Windows 2000 eingeben.

1. Wählen Sie in der Merkmalliste die Option **Windows 2000-Verzeichnis** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Geben Sie im Feld **Basisverzeichnis** den Pfad für das Basisverzeichnis des Benutzers ein. Der angegebene Wert kann lokal oder fern sein. Beispiel für ein Verzeichnis im lokalen Dateisystem: **C:\Basisverzeichnis**. Beispiel für ein Verzeichnis in einem fernen Dateisystem: **\\Server\Users\Basisverzeichnis**.

   Anmerkung: In dem Beispiel für ein Verzeichnis in einem fernen Dateisystem muss das Basisverzeichnis ein vorhandenes Verzeichnis für gemeinsame Nutzung sein und über entsprechende Zugriffsberechtigungen verfügen.

3. Geben Sie im Feld **Laufwerk für lokale Verbindungen** das Laufwerk ein, an das die fernen Verzeichnisse bei der Anmeldung des Benutzers angehängt werden. Die Angabe eines Doppelpunktes nach dem Laufwerkbuchstaben ist optional.

4. Wählen Sie das Kontrollkästchen **Nach Löschen des Benutzers auch Basisverzeichnis löschen** aus, wenn das Basisverzeichnis beim Löschen des Benutzerdatensatzes aus dem Benutzerprofil ebenfalls gelöscht werden soll. Das Verzeichnis wird in diesem Fall erst bei der Verteilung des Profils gelöscht.

5. Geben Sie im Feld **Profilname** den Pfad für das Windows 2000-Benutzerprofil ein. Das Windows 2000-Benutzerprofil definiert die Umgebung, die vom System bei der Benutzeranmeldung geladen wird. Der ferne Pfad muss im Format *Servername**Profilordnername**Profilname* eingegeben werden. Der lokale Pfad muss im Format C:*Verzeichnis**Profilname* eingegeben werden.
6. Geben Sie im Feld **Anmeldeskript** den Pfad für das Anmeldeskript des Benutzers ein.

Windows 2000-Gruppen

Über die Option **Windows 2000-Gruppenzugehörigkeit** können Sie Benutzern Gruppenzugehörigkeiten zuordnen.

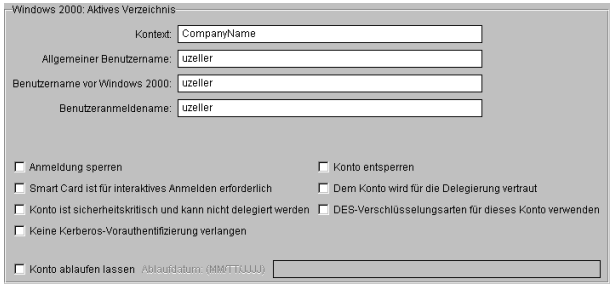
1. Wählen Sie die Option **Windows 2000-Gruppenzugehörigkeit** in der Merkmalliste aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen.

2. Wählen Sie in der Dropdown-Liste **Primärgruppe** die Primärgruppe aus, zu der der Benutzer gehören soll.
3. Geben Sie zusätzliche Gruppen an, indem Sie den Gruppennamen im Feld am unteren Rand der Anzeige im kanonischen Format eingeben (<*Domäne*>/*Kontext1*/*Kontext2*/ . .) . Klicken Sie dann auf die Schaltfläche **Hinzufügen**, die sich links neben dem Feld befindet.

Windows 2000-Anmeldung

Mit der Option **Windows 2000-Anmeldung** können Sie die Anmeldeinformationen für Windows 2000 eingeben.

1. Wählen Sie die Option **Windows 2000-Anmeldung** in der Merkmalliste aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen.



2. Geben Sie im Feld **Kontext** einen Kontext im kanonischen Format ein (*<Domäne>*/*Kontext1*/*Kontext2*/. . .).
3. Geben Sie den allgemeinen Namen des Benutzers im Feld **Allgemeiner Benutzername** ein.
4. Der Benutzername, den Sie im Feld **Benutzername vor Windows 2000** eingeben, muss ein eindeutiger SAM-Kontoname in der Domäne sein. Hierbei handelt es sich um ein Musseingabefeld.
5. Geben Sie im Feld **Benutzeranmeldename** den Anmeldenamen des Benutzers ein. Nur der Name sollte eingegeben werden. Es muss sich um einen eindeutigen Namen in der Domäne handeln. Der daraus resultierende **Principal-Name des Benutzers** hat folgendes Format:

   <Name>@*<Domäne>*

   Anmerkung: In einer typischen Windows 2000-Serverkonfiguration kann sich der Benutzer anmelden, indem er entweder den Benutzernamen vor Windows 2000 oder den Benutzeranmeldenamen verwendet.

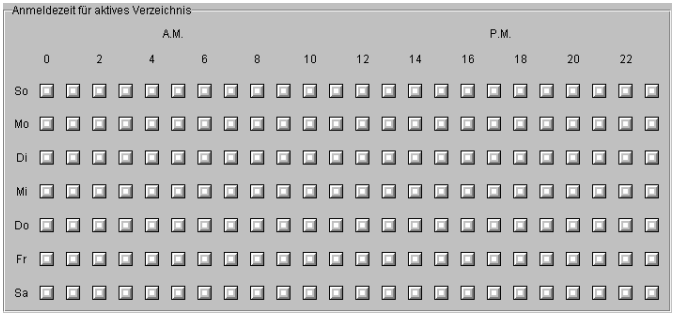
Diese Namen müssen in der Domäne eindeutig sein. Wenn diese Namen nicht eindeutig sind, kann der Benutzerdatensatz nicht verteilt werden.

6. Diese Anzeige enthält Kontrollkästchen zu Angabe von verschiedenen Merkmalen für das Benutzerkonto. Wählen Sie für die zu aktivierenden Funktionen das entsprechende Kontrollkästchen aus.

Windows 2000-Anmeldezeit

Mit der Option **Windows 2000-Anmeldezeit** können Sie die Uhrzeiten festlegen, zu denen sich der betreffende Benutzer unter diesem Benutzerkonto am Netzwerk anmelden kann.

1. Wählen Sie die Option **Windows 2000-Anmeldezeit** in der Merkmalliste aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:

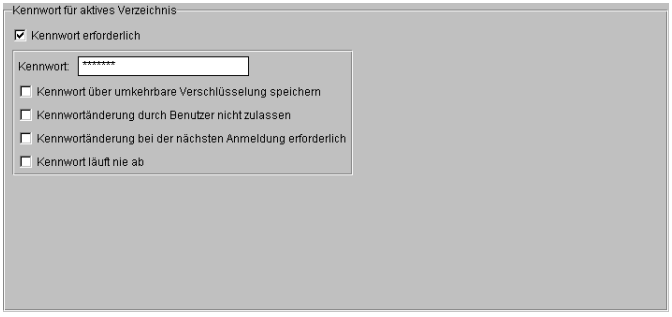


2. Wählen Sie die Uhrzeiten und Tage aus, auf die Sie den Zugriff des Benutzers auf das Netzwerk beschränken möchten, indem Sie die entsprechenden Kontrollkästchen auswählen. Ein ausgewähltes Kontrollkästchen wird dunkel dargestellt (der weiße Punkt ist nicht sichtbar). Erfolgt keine Auswahl, kann sich der Benutzer jederzeit am Netzwerk anmelden.

Windows 2000-Kennwort

Mit der Option **Windows 2000-Kennwort** können Sie das Kennwort des Benutzers festlegen und bestimmte Kenndaten bezüglich dieses Kennworts definieren.

1. Wählen Sie in der Merkmalliste die Option **Windows 2000-Kennwort** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:

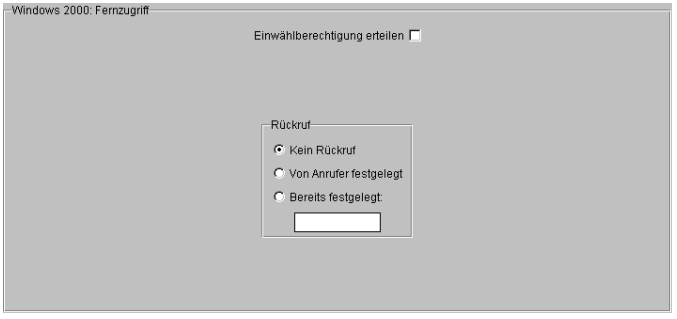


2. Wählen Sie das Kontrollkästchen **Kennwort erforderlich** aus, wenn für dieses Benutzerkonto ein Kennwort erforderlich ist.
3. Geben Sie im Feld **Kennwort** das Kennwort des Benutzers ein.
4. Wählen Sie das Kontrollkästchen **Kennwort über umkehrbare Verschlüsselung speichern** aus, wenn Sie die reversible Verschlüsselung aktivieren möchten.
5. Wählen Sie das Kontrollkästchen **Kennwortänderung durch Benutzer nicht zulassen**, wenn Sie nicht möchten, dass das Kennwort vom Benutzer geändert wird. In diesem Fall muss der Administrator Kennwortänderungen vornehmen.
6. Aktivieren Sie das Kontrollkästchen **Kennwortänderung bei der nächsten Anmeldung erforderlich**, wenn der Benutzer bei der ersten Anmeldung nach Verteilung des Profils das Kennwort ändern soll.
7. Wählen Sie das Kontrollkästchen **Kennwort läuft nie ab** aus, wenn für den Benutzer keine Notwendigkeit einer Kennwortänderung bestehen soll.

Windows 2000-Fernzugriff

Mit der Option **Windows 2000-Fernzugriff** können Sie die Einwählberechtigungen für einen Benutzer festlegen. Diese Berechtigungen gelten nur für RAS-Server (Remote Access Service).

1. Wählen Sie in der Merkmalliste die Option **Windows 2000-Fernzugriff** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen.



2. Wählen Sie das Kontrollkästchen **Einwählberechtigung erteilen** aus, um dem Benutzer den RAS-Zugriff zu ermöglichen.

3. Bei Aktivierung der Windows 2000-RAS-Rückrufoption stellt der Benutzer über einen Anruf eine Verbindung zum RAS-Server her. Der RAS-Server trennt die Verbindung und ruft unmittelbar danach die vorgegebene bzw. die vom Benutzer angegebene Rufnummer zurück. Klicken Sie auf eines der folgenden Optionsfelder, um die Rückrufoption für den Benutzer festzulegen:

   Kein Rückruf

   Die Rückruffunktion ist nicht aktiviert. Der Benutzer kann sich einwählen und erhält unmittelbaren Zugriff auf das System.

Von Anrufer festgelegt

Die vom Benutzer angegebene Rufnummer wird zurückgerufen. Diese Funktion ist ausgesprochen hilfreich für Benutzer, die sich von verschiedenen Standorten aus und unter verschiedenen Rufnummern einwählen.

Bereits festgelegt

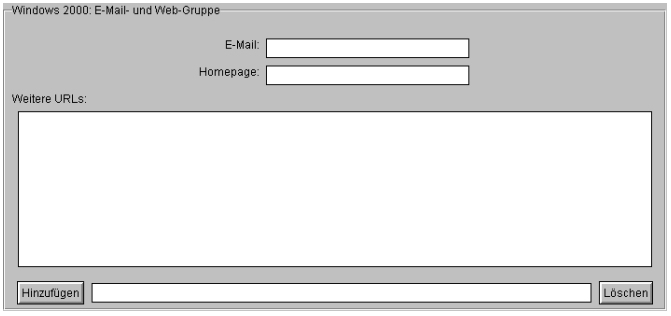
Die angegebene Rufnummer wird zurückgerufen. Diese Option sollte für ferne Computer an festen Standorten, wie beispielsweise das Büro zu Hause, angegeben werden.

Anmerkung: Wird **Kein Rückruf** oder **Von Anrufer festgelegt** aktiviert und ist gleichzeitig im Feld **Bereits festgelegt** noch eine Rufnummer angegeben, kommt es unter Umständen zu Konflikten zwischen den Einträgen im Tivoli-Benutzerprofil und in der RAS-Datenbank auf dem Windows 2000-Server. Dies führt unter Umständen dazu, dass Sie über den Windows 2000-Benutzer-Manager keine neue Rufnummer eingeben können. Dieses Problem kann umgangen werden, indem Sie über die Richtlinie für Gültigkeitsprüfung die Eingabe einer Rufnummer durch den Administrator bzw. das System verhindern, wenn das Kontrollkästchen **Bereits festgelegt** nicht aktiviert ist.

Windows 2000-Webgruppe

Mit der Option **Windows 2000-E-Mail- und -Web-Gruppe** können Sie die Weboptionen für Benutzer festlegen.

1. Wählen Sie die Option **Windows 2000-Web-Gruppe** in der Merkmalliste aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:

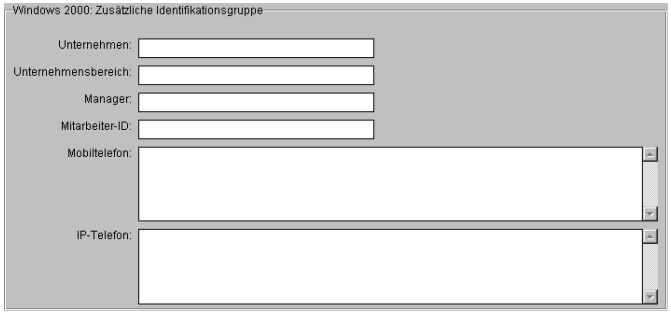


2. Geben Sie im Feld **E-Mail** die E-Mail-Adresse des Benutzers ein.
3. Geben Sie im Feld **Homepage** die URL der Website des Benutzers ein.
4. Geben Sie weitere URLs an, auf die der Benutzer Zugriff haben soll, indem Sie die entsprechende URL im Feld am unteren Rand der Anzeige eingeben und auf die Schalfläche **Hinzufügen**, die sich neben dem Feld befindet, klicken.

Windows 2000 - Zusätzliche Identifikationsgruppe

Mit der Option **Windows 2000 Zusätzliche Identifikationsgruppe** können Sie zusätzliche Benutzerinformationen wie beispielsweise Mitarbeiter-ID, Handynummer etc. angeben.

1. Wählen Sie in der Merkmalliste die Option **Windows 2000 Zusätzliche Identifikationsgruppe** aus.



2. Geben Sie im Feld **Unternehmen** den Firmennamen ein.
3. Geben Sie im Feld **Unternehmensbereich** den Namen der Abteilung, in der der Benutzer arbeitet, ein.
4. Geben Sie im Feld **Manager** den Namen des Vorgesetzten des Benutzers ein.
5. Geben Sie im Feld **Mitarbeiter-ID** die Mitarbeiter-ID des Benutzers ein.
6. Geben Sie in der Liste **Mobiltelefon** die Handynummer des Benutzers ein.
7. Geben Sie in der Liste **IP-Telefon** die IP-Telefonnummer des Benutzers ein.

Informationen zu NetWare-Benutzerkonten

Mit Tivoli SecureWay User Administration können Sie Benutzerkonten für NetWare verwalten. Folgende Informationen können Sie für einen NetWare-Benutzerdatensatz eingeben:

- Anmeldeinformationen
- Anmeldezeiten
- Kennwortinformationen
- Informationen zum Basisverzeichnis
- Informationen zur Netzwerkadresse
- Informationen zur Gruppenzugehörigkeit
- Sicherheitsinformationen
- Informationen zu E-Mail
- Verwaltungsinformationen
- Informationen zum Anmeldeskript
- Informationen zu Speicherbereichseinschränkungen auf Datenträgern
- Informationen zu Workstations

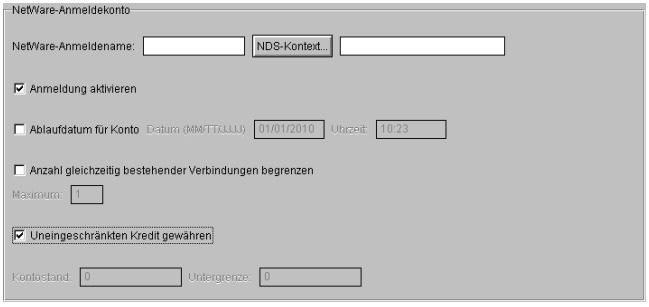
Führen Sie folgende Schritte aus, um Benutzerinformationen für NetWare hinzuzufügen:

1. Wählen Sie in der Dropdown-Liste **Kategorie** die Option **NetWare** aus.
2. Wählen Sie die gewünschte Option in der Merkmalliste aus.

Informationen zur NetWare-Anmeldung

Mit der Option **NetWare-Anmeldung** können Sie die entsprechenden Informationen für NetWare-Anmeldungen eingeben.

1. Wählen Sie in der Merkmalliste die Option **NetWare-Anmeldung** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Geben Sie im Feld **NetWare-Anmeldename** den NetWare-Anmeldenamen des Benutzers ein.

   Anmerkung: NetWare unterstützt Anmeldenamen mit Leerzeichen, Tivoli SecureWay User Administration jedoch nicht. Wenn eine NetWare-Anmelde-ID ein Leerzeichen enthält, muss der Benutzer das Leerzeichen durch ein Unterstreichungszeichen (_) ersetzen, um sich erfolgreich anmelden zu können.

3. Für Konten unter NetWare 4.x und 5.x müssen Sie den Benutzerkontext im Feld **NDS-Kontext** angeben. Der Benutzerkontext ist die Speicherposition des Benutzercontainerobjekts in der Verzeichnisbaumstruktur. Wenn beispielsweise Jon Smith im Unternehmensbereich (**CORPORATE**) der Abteilung Marketing (**MARKETING**) für das Unternehmen NoonTide (**NOON**) tätig ist, lautet sein Kontext **CORPORATE.MARKETING.NOON**-.Geben Sie den Benutzerkontext immer von der niedrigsten zur höchsten Verzeichnisebene an.

   Anmerkung: Wenn Sie keinen NDS-Kontext angeben, wird dieser Benutzer nicht erstellt.

Klicken Sie auf **NDS-Kontext**, um den Dialog **Dienst-Browser für NetWare-Verzeichnisse** anzuzeigen.

a. Klicken Sie doppelt auf einen in der Liste **NetWare-Knoten** angezeigten Knoten. Der Dialog wird aktualisiert, um die NDS-Kontexte anzuzeigen, die dem ausgewählten Knoten zugeordnet sind.

b. Wählen Sie einen Kontext in der Liste **Kontext** aus.

c. Klicken Sie auf **Auswählen und schließen**, um zum Dialog **Benutzermerkmale** zurückzukehren.

4. Wählen Sie das Kontrollkästchen **Anmeldung aktivieren** aus, um die Anmeldung dieses Benutzers zu aktivieren.

5. Wählen Sie das Kontrollkästchen **Ablaufdatum für Konto** aus, um für dieses Benutzerkonto ein Ablaufdatum festzulegen.

   a. Geben Sie im Datumsfeld das Ablaufdatum im Format Monat/Tag/Jahr (*MM/TT/JJJJ*) ein.

   b. Geben Sie im Feld für die Uhrzeit die Ablaufzeit im 24-Stunden-Format (*HHMM*) ein.

   Anmerkung: Die Stunden (*HH*) können entweder durch eine oder zwei Ziffern angegeben werden.

6. Wählen Sie das Kontrollkästchen **Anzahl gleichzeitig bestehender Verbindungen begrenzen** aus, um die Anzahl der gleichzeitig bestehenden Verbindungen für diesen Benutzer zu begrenzen.

   Geben Sie nach Auswahl dieses Kontrollkästchen im Feld **Maximum** die Anzahl der gleichzeitig zulässigen Verbindungen ein.

7. Wählen Sie das Kontrollkästchen **Uneingeschränkten Kredit gewähren** aus, um die NetWare-Kontostände nicht zu verfolgen.

   — ODER —

   a. Geben Sie im Feld **Kontostand** den Kontostand des Benutzers ein. Das ist der Kredit, den der Benutzer zu Beginn des Kontos besitzt.

      Anmerkung: Wenn das Feld **Kontostand** leer bleibt, hat der Benutzer einen Kontostand von Null.

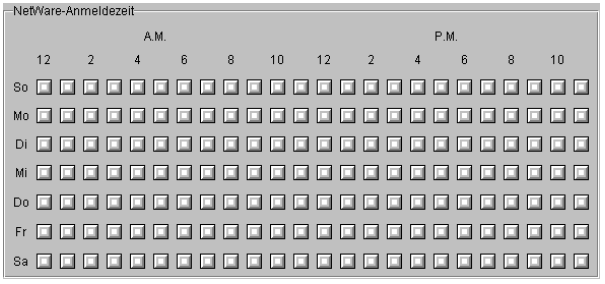
   b. Geben Sie im Feld **Untergrenze** den Mindestsaldo des Benutzers ein. Sobald der Kontostand des Benutzers diese Zahl erreicht, kann der Benutzer die Netzwerkressourcen nicht mehr verwenden. Der Mindestsaldo kann negativ sein, so dass der Benutzer den für den Kontostand gesetzten Wert überschreiten kann.

Anmerkung: Die Leistungsverrechnung von NetWare muss aktiv sein, damit diese Funktionen wirksam sind.

Informationen zur NetWare-Anmeldezeit

Mit der Option **NetWare-Anmeldezeit** können Sie die Uhrzeiten festlegen, zu denen sich ein Benutzer unter einem Konto am Netzwerk anmelden kann. Wenn Sie den Zugriff auf Ihr Netzwerk zu bestimmten Zeiten nicht zulassen möchten, zum Beispiel am Abend, wenn Sie Sicherungskopien auf Band speichern, können Sie verhindern, dass sich Benutzer in dieser Zeit anmelden.

1. Wählen Sie in der Merkmalliste die Option **NetWare-Anmeldezeit** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:

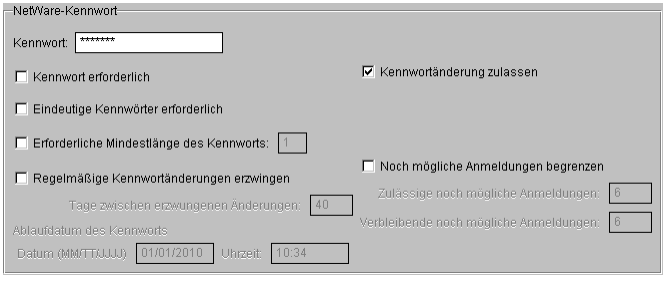


2. Wählen Sie die Uhrzeiten und Tage aus, auf die Sie den Zugriff des Benutzers auf das Netzwerk beschränken möchten, indem Sie die entsprechenden Kontrollkästchen auswählen. Wenn Sie keine Kontrollkästchen auswählen, kann sich der Benutzer jederzeit anmelden.

Informationen zum NetWare-Kennwort

Mit der Option **NetWare-Kennwort** können Sie das Kennwort des Benutzers festlegen und bestimmte Kenndaten bezüglich des Benutzerkennworts definieren.

1. Wählen Sie in der Merkmalliste die Option **NetWare-Kennwort** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Geben Sie im Feld **Kennwort** das Kennwort des Benutzers ein.
3. Wählen Sie das Kontrollkästchen **Kennwort erforderlich** aus, wenn der Benutzer beim Anmelden ein Kennwort angeben soll.

4. Wählen Sie das Kontrollkästchen **Eindeutige Kennwörter erforderlich** aus, wenn der Benutzer eindeutige Kennwörter verwenden soll.
5. Wählen Sie das Kontrollkästchen **Erforderliche Mindestlänge des Kennworts** aus, um die Mindestlänge des Kennworts festzulegen. Geben Sie anschließend die Mindestlänge in das Textfeld ein.
6. Wählen Sie das Kontrollkästchen **Regelmäßige Kennwortänderungen erzwingen** aus, wenn der Benutzer sein Kennwort regelmäßig ändern soll.
   a. Geben Sie im Feld **Tage zwischen erzwungenen Änderungen** die Anzahl der zwischen den Kennwortänderungen liegenden Tage ein.
   b. Geben Sie im Datumsfeld das Datum ein, an dem das aktuelle Kennwort ungültig wird. Geben Sie im Uhrzeitfeld die Uhrzeit für das Datum ein, zu der das aktuelle Kennwort ungültig wird.
7. Wählen Sie das Kontrollkästchen **Kennwortänderung zulassen** aus, wenn der Benutzer die Möglichkeit erhalten soll, das Kennwort zu ändern. Wenn Sie dieses Kontrollkästchen nicht auswählen, steuert der Administrator das Kennwort dieses Benutzers.
8. Wählen Sie das Kontrollkästchen **Noch mögliche Anmeldungen begrenzen** aus, um die Anzahl der noch möglichen Anmeldungen, die dem Benutzer vor Ablauf des Kennworts zur Verfügung stehen, zu begrenzen. Dadurch wird die Anzahl der noch möglichen Anmeldungen begrenzt. Wenn Sie dieses Kontrollkästchen nicht auswählen, werden dem Benutzer standardmäßig noch sechs mögliche Anmeldungen gewährt.

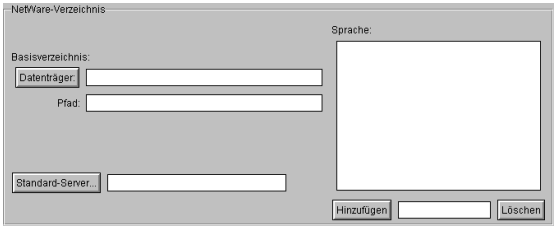
   Geben Sie im Feld **Zulässige noch mögliche Anmeldungen** die Anzahl der noch möglichen Anmeldungen ein.

   Im Feld **Verbleibende noch mögliche Anmeldungen** wird die Anzahl der noch möglichen Anmeldungen angezeigt, die für dieses Benutzerkonto verfügbar sind.

Informationen zum NetWare-Verzeichnis

Über die Option **NetWare-Verzeichnis** können Sie Informationen zu einem Basisverzeichnis eingeben.

1. Wählen Sie in der Merkmalliste die Option **NetWare-Verzeichnis** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Geben Sie im Feld **Datenträger** den Datenträger ein, auf dem sich dieses Basisverzeichnis befindet. Hier müssen Sie den vollständigen NDS-Namen des Datenträgers angeben. Wenn zum Beispiel der Datenträger **SYS** auf dem Server **OLYMPUS** in der NDS-Baumstruktur **NOON** verwendet werden soll, geben Sie **OLYMPUS_SYS.NOON** ein.

   — ODER —

   Klicken Sie auf **Datenträger**, um den Dialog **Dienst-Browser für NetWare-Verzeichnisse** aufzurufen und dort nach einem bestimmten Datenträger zu suchen. Weitere Informationen zu diesem Dialog finden Sie unter „Dienst-Browser für NetWare-Verzeichnisse verwenden” auf Seite 209.

3. Geben Sie im Feld **Pfad** den Pfad für dieses Basisverzeichnis ein.

4. Geben Sie im Feld **Standardserver** den Namen des betreffenden Servers ein, an dem sich dieser Benutzer anmeldet. Hier müssen Sie den vollständigen NDS-Namen für den Server angeben. Wenn zum Beispiel der Server **OLYMPUS** in der NDS-Baumstruktur **NOON** verwendet werden soll, geben Sie **OLYMPUS.NOON** ein. Sie können auch auf **Standardserver** klicken, um den Dialog **Dienst-Browser für NetWare-Verzeichnisse**

anzuzeigen. Einzelheiten zur Verwendung des Dialogs **Dienst-Browser für NetWare-Verzeichnisse** finden Sie in diesem Abschnitt in Schritt 2.

5. Wählen Sie in der Liste mit Sprachen die Sprache aus, in der die NetWare-Nachrichten für diesen Benutzer angezeigt werden sollen.

Informationen zur NetWare-Netzwerkadresse

Mit der Option **NetWare-Netzwerkadresse** können Sie die Workstations einschränken, von denen sich Benutzer am Netzwerk anmelden können.

Die Werte für das erste Element des Arguments **-Aw** können das Format *Wert:restlicheNetzwerkadresse* oder*Wert:Hostname:restliche-Netzwerkadresse* haben.

- Geben Sie für das Netzwerk die Kabelsegmentnummer in 8 hexadezimalen Bytes (Ziffern 0-9, Buchstaben A-F) ein.
- Geben Sie für den Knoten die Netzkartennummer in 12 hexadezimalen Bytes (Ziffern 0-9, Buchstaben A-F) ein.

Da beispielsweise 0 = IPX und 1 = IP gilt, könnte die NetWare-Netzwerkadresseneinschränkung für den Benutzer **utu9232** wie folgt lauten:

-Aw 0:0000002F:FFFFFFFFFFFF

-Aw 1:146.49.7.102

Prüfen Sie die folgenden Wertezuordnungen und -informationen:

IPX/SPX = value 0
: Gibt eine IPX/SPX-Adresse (Internetwork Packet Exchange/Sequence Packet Exchange) an. Wenn alle Knoten in einem Segment gültig sind, geben Sie alle **F**s als Knotenadresse an.

TCP/IP = Wert 1
: Gibt eine Internet Protocol-Adresse an. Geben Sie eine Dezi-

malzahl zwischen 0 und 255 in jedem Feld ein. Die linke Hälfte der Adresse gibt das Netzwerksegment an. Die rechte Hälfte gibt den Computer an.

SDLC = Wert 2

Gibt eine SDLC-Adresse (Synchronous Data Link Control = synchrone Datenübertragungssteuerung) an. Geben Sie einen hexadezimalen Wert (Ziffern 0-9, Buchstaben A-F) in jedem Feld ein.

Ethernet = Wert 3

Gibt eine Ethernet- oder Token-Ring-Adresse an. Geben Sie eine Hexadezimalzahl (Ziffern 0-9, Buchstaben A-F) in jedem Feld ein.

OSI = Wert 4

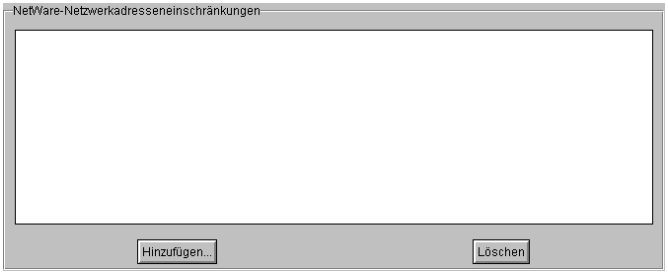
Gibt eine OSI-Adresse (Open Systems Interconnection = Kommunikation offener Systeme) an. Geben Sie die Adresse als hexadezimalen Wert (Ziffern 0-9, Buchstaben A-F) ein.

Appletalk = Wert 5

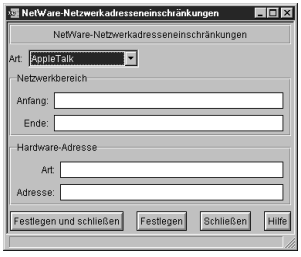
Gibt eine AppleTalk-Adresse an. Geben Sie eine Dezimalzahl in den ersten drei Feldern und eine Hexadezimalzahl (Ziffern 0-9, Buchstaben A-F) im letzten Feld ein. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Hardware.

Führen Sie folgende Schritte durch, um die Netzwerkadresseneinschränkungen festzulegen:

1. Wählen Sie in der Merkmalliste die Option **NetWare-Netzwerkadresse** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Klicken Sie auf **Hinzufügen**, um den Dialog **NetWare-Netzwerkadresseneinschränkungen** anzuzeigen.



3. Wählen Sie in der Dropdown-Liste **Art** die Netzwerkadressenart aus. Sie können zwischen den Adressenarten **AppleTalk**, **Ethernet/Token Ring**, **IPX/SPX**, **OSI**, **SDLC** und **TCP/IP** auswählen.

   - Wenn Sie die Option **AppleTalk** ausgewählt haben, geben Sie in den folgenden Feldern Werte ein:

     Anfang
     Gibt die Anfangszahl des Bereichs gültiger Netzwerknummern an. Eine Netzwerknummer kann eine beliebige Dezimalzahl von 1 bis 65.279 sein.

     Ende Gibt die letzte Zahl des Bereichs gültiger Netzwerknummern an. Eine Netzwerknummer kann eine beliebige Dezimalzahl von 1 bis 65.279 sein.

     Art Gibt einen einstelligen Code an, der einer bestimmten Art von Netzwerkkarte entspricht. AppleTalk unterstützt die folgenden Codes:

     3 Ethernet

     4 ARCNet

     5 Token-Ring

     6 FDDI

     Adresse
     Gibt die Knotenadresse an, die bis zu zwölf hexadezimale Zeichen enthalten kann.

- Wenn Sie die Option **Ethernet/Token Ring** ausgewählt haben, geben Sie Werte in den Feldern **SAP**, **BLOCKID** und **PUID** ein. Informationen zum Festlegen der entsprechenden Werte finden Sie in der Dokumentation zu Ihrer Hardware.
- Geben Sie bei Aktivierung der Option **IPX/SPX** Werte in den folgenden Feldern ein:

  Netzwerk

  Gibt eine Netzwerkzahl an. Eine Netzwerkzahl wird einem Kabelsegment willkürlich zugeordnet, wenn das Netzwerk eingerichtet wird. Sie enthält bis zu acht hexadezimale Zeichen.

  Knoten

  Gibt eine Host-spezifische Zahl an, so wie sie von der Netzwerkplatine festgelegt wurde. Eine Knotenadresse enthält bis zu zwölf hexadezimale Zeichen.

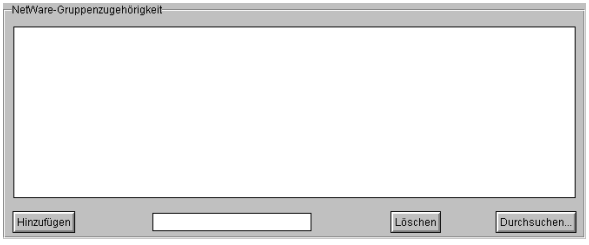
  Damit sich ein Benutzer von allen Knotenadressen im angegebenen Netzwerk anmelden kann, geben Sie die Knotenadresse **FFFFFFFFFFFF** an.
- Geben Sie bei Auswahl der Option **OSI** einen Wert im Feld **OSI-Adresse** ein.
- Geben Sie bei Auswahl der Option **SDLC** Werte in den Feldern **CUA**, **BLOCKID** und **PUID** ein. Informationen zum Festlegen der entsprechenden Werte finden Sie in der Dokumentation zu Ihrer Hardware.
- Geben Sie bei Auswahl der Option **TCP/IP** die IP-Adresse ein. In jedem Feld einer IP-Adresse muss eine Zahl aus dem Bereich zwischen 0 und 255 stehen.

4. Klicken Sie auf **Festlegen und schließen**, um die Netzwerkadresseneinschränkungen festzulegen und zum Dialog **Benutzermerkmale** zurückzukehren.

Informationen zur NetWare-Gruppenzugehörigkeit

Mit der Option **NetWare-Gruppenzugehörigkeit** können Sie NetWare-Gruppenzugehörigkeiten für einen Benutzer definieren.

1. Wählen Sie in der Merkmalliste die Option **NetWare-Gruppenzugehörigkeit** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Geben Sie den Namen der Gruppe ein, zu der der Benutzer gehört, und klicken Sie auf **Hinzufügen**. Die Gruppe wird daraufhin der entsprechenden Liste hinzugefügt. Wiederholen Sie diesen Schritt, so oft es erforderlich ist.

Geben Sie z. B. zum Hinzufügen der Gruppe **NOON GROUP** zum Noon-Kontext **NOON_GROUP.NOON** ein, oder suchen Sie die Gruppe mit der Option **Durchsuchen**, so wie Sie die Schaltfläche **Durchsuchen** von NDS bei einer NetWare-Anmeldung verwenden.

Informationen zur NetWare-Sicherheit

Mit der Option **NetWare-Sicherheit** können Sie die Sicherheitsstufe eines Benutzers oder einer Gruppe so festlegen, dass diese mit der Sicherheitsstufe eines anderen angegebenen Benutzers bzw. einer anderen angegebenen Gruppe übereinstimmt.

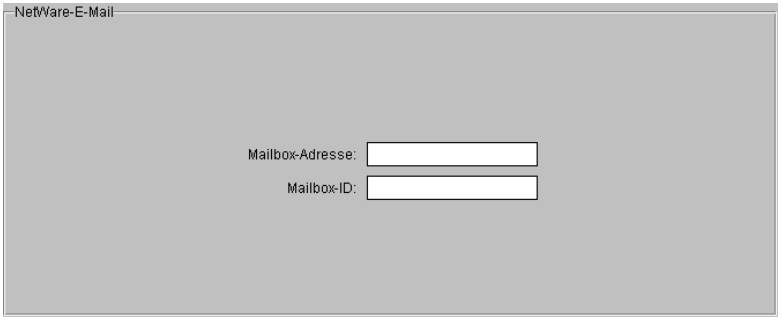
1. Wählen Sie in der Merkmalliste die Option **NetWare-Sicherheit** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:

2. Geben Sie den Anmeldenamen des Benutzers oder den Namen der Gruppe ein, dessen bzw. deren Sicherheitsstufe Sie für diesen Benutzer bzw. diese Gruppe übernehmen möchten, und klicken Sie auf **Hinzufügen**.

Informationen zu NetWare-E-Mail

Mit der Option **NetWare-E-Mail** können Sie die Mailbox-Adresse und die Mailbox-ID des Benutzers definieren.

1. Wählen Sie in der Merkmalliste die Option **NetWare-E-Mail** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:

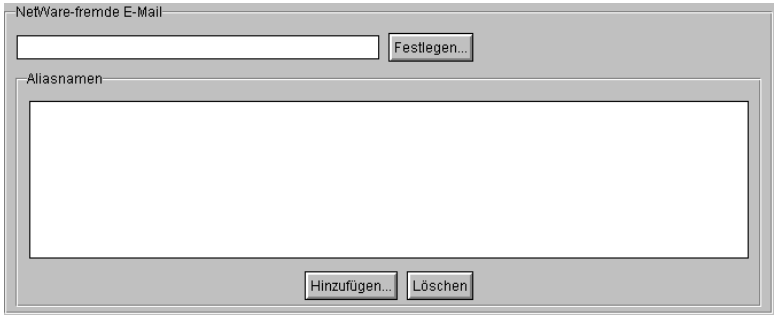


2. Geben Sie im Feld **Mailbox-Adresse** den Namen des Nachrichtenservers ein, auf dem sich die Mailbox des Benutzers befindet.
3. Geben Sie im Feld **Mailbox-ID** die eindeutige Mailbox-ID des Benutzers ein. Mit dieser ID kann die Mailbox des Benutzers in der NetWare-Nachrichtendatenbank lokalisiert werden.

Informationen zu NetWare-fremden E-Mail-Adressen

Mit der Option **NetWare-fremde E-Mail** können Sie externe E-Mail-Adressen für einen Benutzer definieren.

1. Wählen Sie in der Merkmalliste die Option **NetWare-fremde E-Mail** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Klicken Sie zum Hinzufügen einer Adressenart zur Liste **Aliasnamen** auf **Hinzufügen**. Tivoli SecureWay User Administration öffnet den Dialog **NetWare-fremde E-Mail**.

3. Wählen Sie in der Dropdown-Liste **Auswählen...** eine Option aus. Wenn die gewünschte Option nicht aufgeführt ist, können Sie diese im Feld **Art** eingeben.
4. Geben Sie im Feld **Adresse** eine Adresse ein.
5. Klicken Sie auf **Hinzufügen und schließen**, um diesen Dialog zu schließen und die Adresse der Liste **Aliasnamen** hinzuzufügen.

6. Wählen Sie in der Liste **Aliasnamen** einen Namen aus, und klicken Sie anschließend auf **Festlegen**, um den Dialog **NetWare-fremde E-Mail** anzuzeigen. In diesem Dialog können Sie eine fremde E-Mail-Adresse festlegen.

7. Wählen Sie in der Dropdown-Liste **Auswählen...** eine Option aus. Wenn die gewünschte Option nicht aufgeführt ist, können Sie diese im Feld **Art** eingeben.
8. Geben Sie im Feld **Adresse** eine Adresse ein.
9. Klicken Sie auf **Festlegen und schließen**, um diesen Dialog zu schließen und die Adresse dem Adressfeld hinzuzufügen.

Informationen zu NetWare-Anmeldeskripts

Mit der Kategorie **NetWare-Anmeldeskript** können Sie das Anmeldeskript für einen NetWare-Benutzer bearbeiten und diesen einem Anmeldeprofil zuordnen.

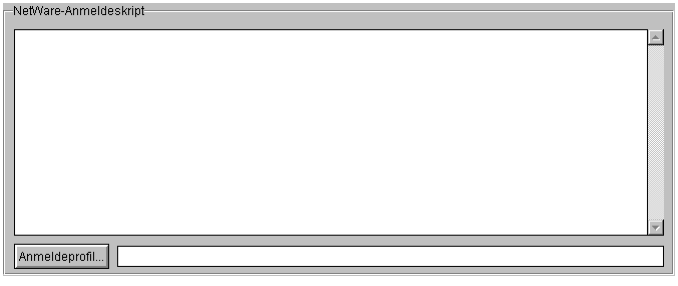
Bei der Anmeldung eines Benutzers in einem NetWare-Konto können von NetWare mehrere Anmeldeskripts ausgeführt werden. Dazu gehören Kontext-, Container-, Anmeldeprofil- und die benutzerspezifischen Anmeldeskripts. Kontext-, Container- und Anmeldeprofilskripts legen die Anmeldekenndaten fest, die für eine Vielzahl von Benutzern gelten. Zusammen setzen diese Skripts in der Regel die Informationen zur Umgebung und steuern die Anzeige von Anmeldenachrichten. Nach Ausführung dieser Skripts wird von NetWare das Anmeldeskript des Benutzers ausgeführt; ist keine vorhanden, kommt ein Standardskript zur Ausführung.

Da der Großteil der Einstellungen, die dem Benutzer das Arbeiten an einer NetWare-Workstation ermöglichen, von den Kontext-, Container- und Anmeldeprofilskripts festgelegt werden, enthält das Anmeldeskript in der Regel nur sehr wenige Befehle. Dazu gehören beispielsweise Druckoptionen sowie ein Benutzername für die E-Mail-Funktion. Daher wird von Tivoli SecureWay User Administration die Größe der Benutzeranmeldeskripts auf 4 KB beschränkt.

Anmerkung: Der Inhalt von NetWare-Anmeldeprofilen wird nicht von Tivoli SecureWay User Administration gesteuert. Daher können Standard-, Container-, Kontext- oder Anmeldeprofilskripts nicht mit Tivoli SecureWay User Administration bearbeitet werden.

Unterhalb der Beschriftung **NetWare-Anmeldeskript** befindet sich ein Textfeld, das ein Benutzeranmeldeskript enthalten kann. (Es handelt sich hier nicht um eine leere Liste.) In dieses Textfeld können mehrere Zeilen (auch mit Leerzeilen) eingegeben werden.

1. Wählen Sie in der Merkmalliste die Option **NetWare-Anmeldeskript** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Geben Sie im Textfeld das Anmeldeskript für den Benutzer ein. Das Anmeldeskript für einen Benutzer sollte nur Befehle enthalten, die weder in Container- noch in Anmeldeprofilskripts eingegeben werden können.

Anmerkung: Die Syntax der Anmeldeskripts wird von Tivoli SecureWay User Administration nicht auf Richtigkeit überprüft. Allerdings wird die Größe des Skripts durch die Richtlinie für Gültigkeitsprüfung auf 4 KB beschränkt.

3. Geben Sie in dem kleinen Textfeld Name und Pfad eines NetWare-Anmeldeprofils ein.

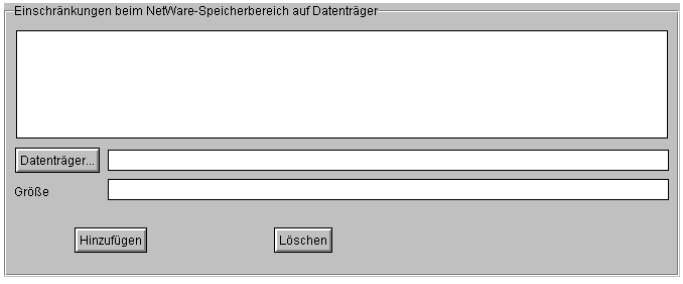
   — ODER —

   Klicken Sie auf **Anmeldeprofil**, um den Dialog **Dienst-Browser für NetWare-Verzeichnisse** aufzurufen und dort nach einem bestimmten Anmeldeprofil zu suchen. Weitere Informationen zu diesem Dialog finden Sie unter „Dienst-Browser für NetWare-Verzeichnisse verwenden” auf Seite 209.

Informationen zur NetWare-Speicherplatz-beschränkung auf Datenträgern

Mit den NetWare-Speicherplatzeinschränkungen auf Datenträgern wird der für Benutzer zulässige Plattenspeicherplatz eingeschränkt. Erfolgen keine Angaben, wird der benutzerspezifische Plattenspeicherplatz eines Datenträgers nur durch die physikalische Kapazität des Datenträgers eingeschränkt.

1. Wählen Sie in der Merkmalliste die Option für die Einschränkung von NetWare-Speicherbereich auf Datenträgern aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Geben Sie den vollständigen Namen des Datenträgers ein, für den Speicherplatzeinschränkungen festgelegt werden sollen.

   — ODER —

   Klicken Sie auf **Datenträger**, um den Dialog **Dienst-Browser für NetWare-Verzeichnisse** aufzurufen und dort nach einem bestimmten Datenträger zu suchen. Weitere Informationen zu diesem Dialog finden Sie unter „Dienst-Browser für NetWare-Verzeichnisse verwenden” auf Seite 209.

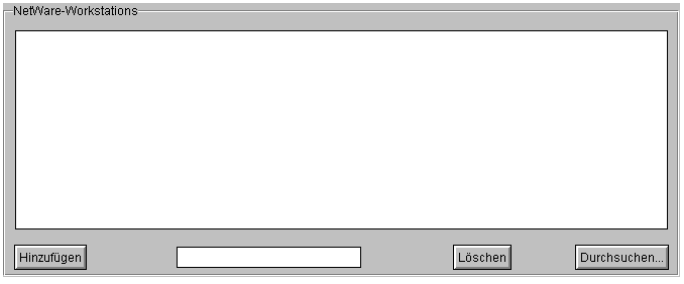
3. Geben Sie den Plattenspeicherplatz (in KB) ein, der dem Benutzer auf dem angegebenen Datenträger zugewiesen wird. Zulässig sind Werte zwischen 0 und 134.217.728 KB; die angegebene Zahl muss durch vier teilbar sein; ist dies nicht der Fall, wird die Angabe auf einen durch vier teilbaren Wert abgerundet. Bei Angabe von Null verfügt der Benutzer über keinen Schreibzugriff auf den Datenträger.

Informationen zu NetWare-Workstations

Die Kategorie **NetWare-Workstations** kann auf Systemen verwendet werden, auf denen Administratoren das Workstation-Objekt einer NDS-Baumstruktur unter Verwendung von NetWare ZENworks und Workstation-Verwaltungskomponenten hinzugefügt haben.

Workstation-Objekte ermöglichen eine konsistente und effiziente ferne Verwaltung von Workstations. Der Administrator kann verschiedene verwaltungstechnische Aufgaben zur Unterstützung von Benutzer oder Gruppen ausführen, wie beispielsweise die Verteilung von Anwendungen, die Einsatzplanung von Programmen oder die Einstellung von Clientkonfigurationen.

1. Wählen Sie in der Merkmalliste die Option **NetWare-Workstations** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Geben Sie den Namen einer NetWare-Workstation ein, und klicken Sie auf **Hinzufügen**. Der Name der Workstation wird der Liste hinzugefügt. Wiederholen Sie diesen Schritt, so oft es erforderlich ist.

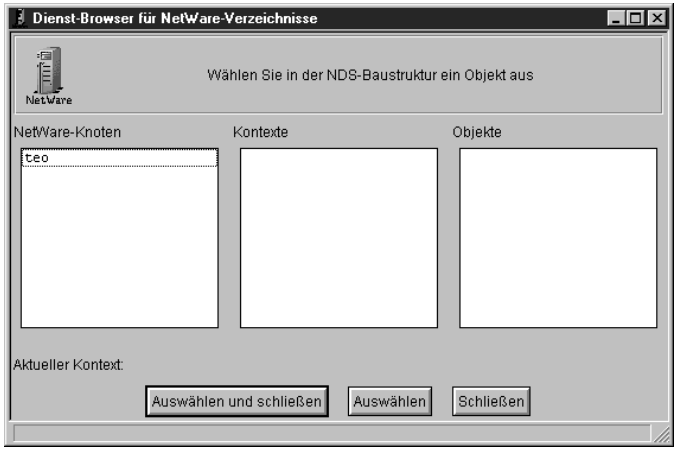
   — ODER —

   Klicken Sie auf **Durchsuchen**, um den Dialog **Dienst-Browser für NetWare-Verzeichnisse** aufzurufen und dort nach einer bestimmten Workstation zu suchen. Weitere Informationen zu diesem Dialog finden Sie unter „Dienst-Browser für NetWare-Verzeichnisse verwenden” auf Seite 209.

Dienst-Browser für NetWare-Verzeichnisse verwenden

In vielen der NetWare-Anzeigen kann der Dienst-Browser für NetWare-Verzeichnisse über eine entsprechende Schaltfläche aufgerufen werden. Mit diesem Browser können Sie NetWare-Objekte auswählen, indem Sie einen Knoten oder einen bzw. mehrere Kontexte durchsuchen.

Bei Klicken auf diese Schaltfläche wird folgender Dialog angezeigt:



1. Klicken Sie doppelt auf einen in der Liste **NetWare-Knoten** angezeigten Knoten. Der Dialog wird aktualisiert und zeigt in der Liste **Kontexte** die vorhandenen Kontexte an.
2. Klicken Sie doppelt auf eine Option in der Liste **Kontexte**. Daraufhin wird in der Liste **Objekte** eine Reihe von Objekten angezeigt. Wenn der von Ihnen ausgewählte Kontext untergeordnete Kontexte enthält, werden diese in der Liste **Kontexte** aufgeführt. Wiederholen Sie diesen Schritt, bis Sie den Kontext finden, der das gewünschte Objekt enthält.
3. Wählen Sie dieses Objekt in der Liste **Objekte** aus.
4. Klicken Sie auf **Auswählen und schließen**, um zum Dialog **Benutzermerkmale** zurückzukehren.

Informationen zu UNIX-Benutzerkonten

Mit Tivoli SecureWay User Administration können Sie Informationen zu UNIX-Benutzerkonten eingeben. Folgende Informationen können Sie für einen Benutzerkontodatensatz unter UNIX eingeben:

- Anmeldeinformationen
- Kennwortinformationen
- Informationen zum Basisverzeichnis
- E-Mail-Informationen

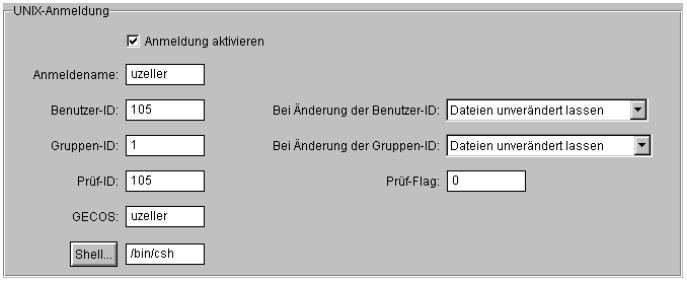
Führen Sie folgende Schritte aus, um UNIX-Benutzerinformationen hinzuzufügen:

1. Wählen Sie in der Dropdown-Liste **Kategorie** die Option **UNIX** aus.
2. Wählen Sie die gewünschte Option in der Merkmalliste aus.

Informationen zur UNIX-Anmeldung

Mit der Option **UNIX-Anmeldung** können Sie allgemeine Kenndaten eines UNIX-Benutzerkontos eingeben.

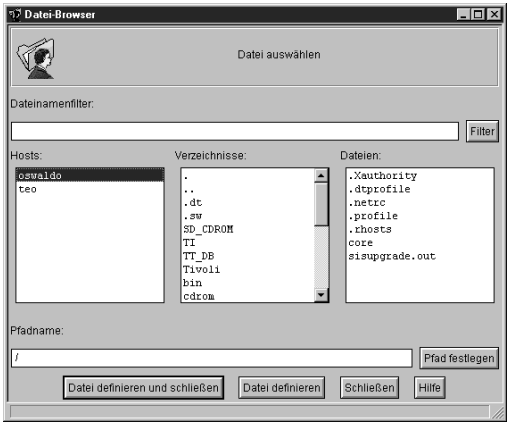
1. Wählen Sie in der Merkmalliste die Option **UNIX-Anmeldung** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Wählen Sie das Kontrollkästchen **Anmeldung aktivieren** aus, um die Anmeldung dieses Benutzers zu aktivieren.

3. Geben Sie im Feld **Anmeldename** den Anmeldenamen des Benutzers ein.
4. Geben Sie im Feld **Benutzer-ID** die Benutzeridentifikationsnummer (UID) für diesen Benutzer ein.
5. Wählen Sie in der Dropdown-Liste **Bei Änderung der Benutzer-ID** die entsprechende Option aus. Die folgenden Optionen sind verfügbar:
   - **Dateien unverändert lassen**
   - **Besitzer-ID der Dateien ändern**
6. Geben Sie im Feld **Gruppen-ID** die ID oder den Namen des Benutzers für die Primärgruppe ein.
7. Wählen Sie in der Dropdown-Liste **Bei Änderung der Gruppen-ID** die entsprechende Option aus. Die folgenden Optionen sind verfügbar:
   - **Dateien unverändert lassen**
   - **Besitzer-ID der Dateien ändern**
8. Geben Sie im Feld **Prüf-ID** die Prüf-ID des Benutzers ein. Mit dem Feld **Prüf-ID** können Sie eine wirklich eindeutige Kennung für einen Benutzerdatensatz eingeben.

   Anmerkung: Die Informationen in diesem Feld sind HP-UX-spezifisch und werden nur im Feld **u_auditid** des Benutzereintrags in der gesicherten und geschützten Kennwortdatenbank von HP-UX 10.*x* und HP-UX 11.*x* eingefügt.
9. Geben Sie im Feld **GECOS** den tatsächlichen Namen des Benutzers ein.
10. Klicken Sie auf **Shell...**, um den Dialog zum Auswählen des Pfads der Anmelde-Shell anzuzeigen.



a. Klicken Sie in der Liste **Hosts** doppelt auf den entsprechenden Server. Tivoli SecureWay User Administration zeigt eine Liste mit Verzeichnissen in der Liste **Verzeichnisse** an.

b. Klicken Sie in der Liste **Verzeichnisse** doppelt auf das Verzeichnis, das die Shell-Interpreter-Befehle enthält. Tivoli SecureWay User Administration zeigt eine Liste mit Dateien in der Liste **Dateien** an.

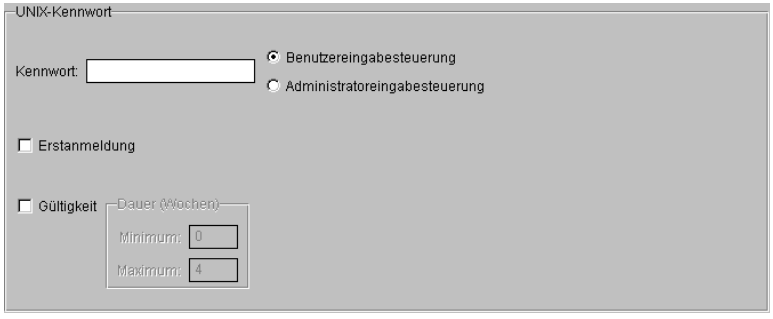
c. Wählen Sie in der Liste **Dateien** die Datei aus, die den Shell-Interpreter darstellt, der für dieses Benutzerkonto verwendet werden soll.

d. Klicken Sie auf **Datei definieren und schließen**, um diesen Pfad dem Feld **Shell...** hinzuzufügen und den Dialog zum Auswählen des Pfads der Anmelde-Shell zu schließen.

Informationen zum UNIX-Kennwort

Mit der Option **UNIX-Kennwort** können Sie das Kennwort des Benutzers festlegen und bestimmte Kenndaten bezüglich des Benutzerkennworts definieren.

1. Wählen Sie in der Merkmalliste die Option **UNIX-Kennwort** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Geben Sie im Feld **Kennwort** das Kennwort des Benutzers ein.
3. Wählen Sie das Optionsfeld **Benutzereingabesteuerung** aus, damit der Benutzer das Kennwort steuern kann.

   — ODER —

   Wählen Sie das Optionsfeld **Administratoreingabesteuerung** aus, damit der Administrator das Kennwort des Benutzers steuern kann.
4. Wählen Sie das Kontrollkästchen **Erstanmeldung** aus, damit Kennwörter nur für die Erstanmeldung gültig sind. Bei Auswahl des Kontrollkästchens **Erstanmeldung** wird der Benutzer bei seiner nächsten Anmeldung nach der Verteilung des Benutzerprofils aufgefordert, sein Kennwort zu ändern.
5. Wählen Sie das Kontrollkästchen **Gültigkeit** aus, um die Kennwortgültigkeitsdauer zu begrenzen. Wenn dieses Kontrollkästchen ausgewählt ist, wird ein Haken darin angezeigt.
   a. Geben Sie im Feld **Minimum** die Mindestgültigkeitsdauer des Kennworts ein.
   b. Geben Sie im Feld **Maximum** die maximale Gültigkeitsdauer des Kennworts ein.

Informationen zum UNIX-Verzeichnis

Mit der Option **UNIX-Verzeichnis** können Sie das Basisverzeichnis festlegen und bestimmte Kenndaten bezüglich des Basisverzeichnisses definieren.

Unterstützung für UNIX-Basisverzeichnisse

Tivoli User Administration unterstützt zwei Arten von UNIX-Basisverzeichnissen:

Lokal an Host

Erstellt auf jedem Endpunkt und verwalteten Knoten, der eine Subskription für das Benutzerprofil einrichtet ist, ein Basisverzeichnis für den Benutzer. Aus diesem Grund enthalten möglicherweise alle subskribierenden Maschinen Hunderte von Basisverzeichnissen, eines für jeden im Benutzerprofil definierten Benutzer.

Fern angehängt

Das Basisverzeichnis ist auf einem NFS-Server gespeichert. Alle subskribierenden Endpunkte und verwalteten Knoten werden an das Dateisystem, das das Basisverzeichnis enthält, angehängt.

Wenn es sich bei dem NFS-Server um einen verwalteten Knoten handelt, verwendet Tivoli SecureWay User Administration Services, die von Tivoli Management Framework zur Verfügung gestellt werden, um alle Operationen, die für das Erstellen und Unterstützen von fern angehängten UNIX-Basisverzeichnissen erforderlich sind, auszuführen. Wenn es sich bei dem NFS-Server nicht um eine Tivoli-verwaltete Ressource handelt, muss das Konto 'root' auf den TMR-Server über Schreibzugriff auf das Dateisystem verfügen.

In der folgenden Tabelle sind die Aktionsarten aufgeführt, die Tivoli User Administration für lokale und fern angehängte Basisverzeichnisse ausführen kann:

Aktion	Wird für lokale Basisverzeichnisse unterstützt	Wird für ferne Basisverzeichnisse unterstützt
Verzeichnis erstellen	Ja	Ja
Verzeichnis löschen	Ja	Ja
Verzeichnis verschieben	Ja	Ja
Verzeichnis kopieren	Ja	Ja

Aktion	Wird für lokale Basisverzeichnisse unterstützt	Wird für ferne Basisverzeichnisse unterstützt
UID bzw. GID des Benutzers ändern	Ja	Ja
Verzeichnisart ändern (lokal oder fern)	Nein	Nein
Bei Erstellung eines Benutzerdatensatzes: mehrere Standarddateien aus einem anderen Verzeichnis auf verwalteten Knoten und Endpunkten kopieren	Ja für verwaltete Knoten; Nein für Endpunkte	Ja
Standarddateien auf verwalteten Knoten und Endpunkten mit dem Befehl **wupdhdir** aktualisieren	Nein	Ja
Bei Erstellung eines Benutzerdatensatzes: mehrere Standarddateien aus einem anderen Verzeichnis in NIS kopieren	Nein	Ja
Standarddateien in NIS mit dem Befehl **wupdhdir** aktualisieren	Nein	Ja

UNIX-Basisverzeichnisse erstellen

Basisverzeichnisse werden von Tivoli SecureWay User Administration erst nach Verteilung des Profils erstellt. Außerdem beeinflussen die Art des Basisverzeichnisses und die Art der Verteilung den Zeitpunkt der Erstellung des Basisverzeichnisses.

Wenn Sie einen Benutzerdatensatz mit der ausgewählten Basisverzeichnisart **Lokal an Host** an einen anderen Profilmanager (keinen Endpunkt) verteilen, wird Tivoli SecureWay User Administration dieses Verzeichnis nicht erstellen.

Wenn Sie diesen Datensatz an den Endpunkt verteilen, wird das Basisverzeichnis erstellt, nachdem das Benutzerkonto der Datei **/etc/passwd** hinzugefügt wurde.

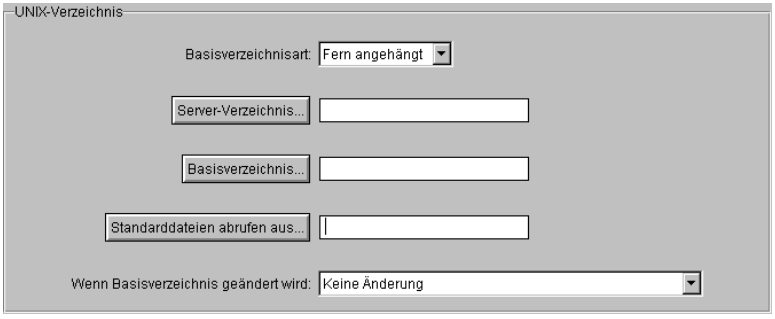
Wenn Sie einen Benutzerdatensatz mit der ausgewählten Basisverzeichnisart **Fern angehängt** an einen anderen Profilmanager (keinen Endpunkt) verteilen, erstellt Tivoli SecureWay User Administration das neue Basisverzeichnis, fügt allerdings den Benutzer nicht der Datei **/etc/passwd** hinzu. Wenn Sie diesen Datensatz an den Endpunkt verteilen, wird der Benutzer der Datei **/etc/passwd** hinzugefügt.

Wenn das Basisverzeichnis, das dem Benutzerkonto zugeordnet ist, nicht bereits bei einer Verteilung auf der nächsten Ebene erstellt wurde, wird es automatisch von Tivoli SecureWay User Administration erstellt.

Die Standardzugriffsrechte eines UNIX-Basisverzeichnisses, das von Tivoli SecureWay User Administration erstellt wurde, lauten **drwx------**. Die Zugriffsrechte werden durch die Standardwertegruppe **umask** definiert. Wenn Sie andere Standardzugriffsrechte benötigen, müssen Sie diese Standardwertegruppe ändern, bevor Sie dem Profil Datensätze hinzufügen. Weitere Informationen zur Handhabung von Standardwertegruppen finden Sie unter „Standardwertegruppen definieren” auf Seite 132.

Sie können ein Benutzerprofil mit UNIX-Benutzerkonten verteilen, deren Basisverzeichnisse von einem nicht von TME verwalteten NFS-Server aus verfügbar sind. Zum Ändern dieser Basisverzeichnisse bzw. zum Erstellen neuer Basisverzeichnisse muss das Konto **root** auf dem TME-Server allerdings über Schreibzugriff auf das NFS-Dateisystem verfügen.

1. Wählen Sie in der Merkmalliste die Option **UNIX-Verzeichnis** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



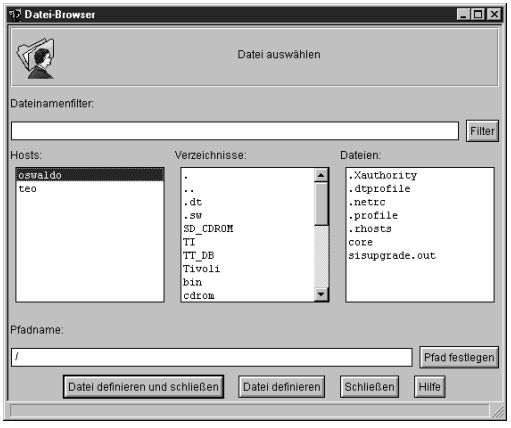
2. Wählen Sie in der Dropdown-Liste **Basisverzeichnisart** die Art des Basisverzeichnisses für den Benutzer aus. Die folgenden Optionen sind verfügbar:

   Keine Gibt an, dass für dieses Benutzerkonto kein Basisverzeichnis vorhanden ist.

   Lokal an Host
   Gibt an, dass sich das Basisverzeichnis auf dem System des Benutzers befindet. Falls Sie diese Option auswählen, wird das lokale Basisverzeichnis erstellt, wenn das Profil an die Systemdateien der Subskribenten verteilt wird.

   Fern angehängt
   Gibt an, dass sich das Basisverzeichnis auf einem angehängten Dateiserver befindet. Falls Sie diese Option auswählen, wird das ferne Basisverzeichnis erstellt, wenn das Profil an Subskribenten verteilt wird.

3. Wenn Sie die Basisverzeichnisart **Fern angehängt** ausgewählt haben, klicken Sie auf **Serververzeichnis**, um den Dialog **Datei-Browser** anzuzeigen.



   a. Klicken Sie in der Liste **Hosts** doppelt auf den entsprechenden Server. Tivoli SecureWay User Administration zeigt die verfügbaren Verzeichnisse in der Liste **Verzeichnisse** an.

   b. Klicken Sie doppelt auf das entsprechende Verzeichnis in der Liste **Verzeichnisse**.

   c. Klicken Sie auf **Datei definieren und schließen**, um diesen Pfad als das Serververzeichnis hinzuzufügen und den Dialog zu schließen.

4. Wenn Sie die Basisverzeichnisart **Lokal an Host** oder **Fern angehängt** ausgewählt haben, klicken Sie auf **Basisverzeichnis**, um den Dialog **Datei-Browser** anzuzeigen. Informationen zur Verwendung dieses Dialogs finden Sie in diesem Abschnitt in Schritt 3.

5. Klicken Sie auf **Standarddateien abrufen aus**, um den Dialog **Datei-Browser** anzuzeigen. Informationen zur Verwendung dieses Dialogs finden Sie in diesem Abschnitt in Schritt 3.
6. Wählen Sie zum Editieren eines vorhandenen Basisverzeichnisses eine der folgenden Optionen in der Dropdown-Liste **Wenn Basisverzeichnis geändert wird** aus:

   Keine Änderung
   Zeigt an, dass die Merkmale eines vorhandenen Basisverzeichnisses nicht geändert werden.

   Neues Basisverzeichnis erstellen
   Richtet ein neues Verzeichnis ein. Dieses Verzeichnis enthält nur die Dateien, die sich in dem Verzeichnis befinden, das im Feld **Standarddateien abrufen aus** ausgewählt wurde.

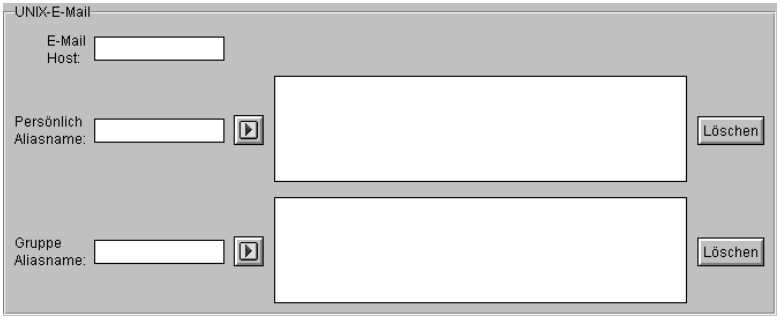
   Inhalt aus altem Basisverzeichnis in neues Basisverzeichnis kopieren
   Kopiert alle Dateien, Verzeichnisse und symbolische Verbindungen in das neue Basisverzeichnis. Verwenden Sie diese Option, wenn Sie ein Archiv des bisherigen Basisverzeichnisses beibehalten möchten.

   Inhalt aus altem Basisverzeichnis in neues Basisverzeichnis verschieben
   Verschiebt alle Dateien, Verzeichnisse und symbolische Verbindungen in das neue Basisverzeichnis.

UNIX-E-Mail

Mit der Option **UNIX-E-Mail** können Sie Informationen bezüglich der UNIX-E-Mail-Adresse des Benutzers eingeben.

1. Wählen Sie in der Merkmalliste die Option **UNIX-E-Mail** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Geben Sie im Feld **E-Mail Host** den Namen des Systems ein, auf dem der Benutzer seine E-Mail empfangen soll.
3. Geben Sie im Feld **Persönlich Aliasname** alle persönlichen E-Mail-Aliasnamen für den Benutzer ein. Klicken Sie nach Eingabe eines Aliasnamen auf den Rechtspfeil, um den Namen in die Liste mit den persönlichen Aliasnamen zu verschieben.
4. Geben Sie im Feld **Gruppe Aliasname** Aliasnamen für E-Mail-Gruppen ein, zu denen der Benutzer gehört. Klicken Sie nach Eingabe eines Aliasnamen auf den Rechtspfeil, um den Namen in die Liste **Gruppe Aliasname** zu verschieben.

7

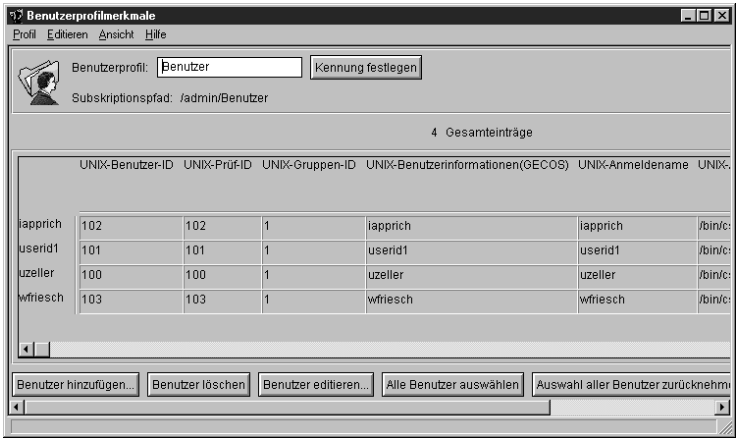
Benutzerdatensätze verwalten

In diesem Kapitel erfahren Sie, wie Benutzerdatensätze verwaltet werden. Typische Tasks sind:

- Nach Benutzerdatensätzen suchen
- Benutzerdatensätze editieren
- Benutzerdatensätze zusammenfügen
- Benutzerdatensätze kopieren
- Benutzerdatensätze verschieben
- Benutzerdatensätze löschen
- Benutzerdatensätze formatieren
- Benutzerdatensätze aus Tivoli entfernen
- Benutzerdatensätze anhand der Richtlinien überprüfen
- Benutzerdatensätze an Subskribenten verteilen
- Gruppendatensätze mit der Tivoli-Datenbank synchronisieren

Sie sollten mit den in „Einführung in die Benutzer- und Gruppenverwaltung” auf Seite 1 aufgeführten Konzepten vertraut sein, bevor Sie mit der Ausführung dieser Tasks beginnen.

Die meisten Tasks zur Verwaltung von Benutzerdatensätzen können Sie im Fenster **Benutzerprofilmerkmale** ausführen.



Mit diesem Profilfenster, wie mit anderen profilbasierten Anwendungen von Tivoli, können Sie Benutzerdatensätze erstellen, editieren und löschen. Außerdem können Sie das Profilverhalten editieren.

Tivoli SecureWay User Administration stellt Ihnen ein Tool zum Suchen nach Benutzern zur Verfügung. Anstatt manuell in Profilmanagern oder Profilen nach einem Benutzer zu suchen, können Sie mit der Benutzersuchfunktion den Benutzer automatisch suchen.

In Tivoli SecureWay User Administration ist für die Kommunikation mit einem NetWare-NDS-Endpunkt die Ausführung des Befehls **wsetnds** erforderlich. Mit diesem Befehl kann sich die Anwendung an der NetWare-NDS-Baumstruktur anmelden. (Da NetWare 3.**x** keine NDS-Baumstrukturen verwendet, müssen Sie den Befehl **wsetnds** nicht ausführen, um mit von NetWare 3.**x** verwalteten Knoten zu kommunizieren.) Sie müssen diesen Befehl für jede von Ihnen verwaltete NDS-Baumstruktur ausführen. Wenn Sie diesen Befehl ausgeführt haben, müssen Sie ihn nicht erneut ausführen, es sei denn, Sie ändern den Anmeldenamen oder das Kennwort des angegebenen Kontos.

Allgemeine Vorgänge für Benutzerdatensätze

Nachdem das Benutzerprofil erstellt und mit Benutzerdaten gefüllt wurde, werden Sie hauptsächlich folgende Vorgänge ausführen: Suchen, Editieren und Löschen von Benutzerdatensätzen und Verteilen von Benutzerprofilen. Weitere Informationen finden Sie in den folgenden Abschnitten:

- Benutzerdatensätze erstellen
- Benutzerdatensätze suchen
- Benutzerdatensätze anzeigen
- Benutzerdatensätze editieren
- Benutzerdatensätze löschen
- Benutzerdatensätze formatieren
- Gruppenprofile an Subskribenten verteilen

Benutzerdatensätze suchen

Auch bei einer steigenden Anzahl von Benutzerkonten, die von Tivoli SecureWay User Administration verwaltet werden, können Sie mit der Benutzersuchfunktion schnell durch Ihre Benutzerprofile navigieren und Kontoverwaltungsfunktionen effizient ausführen. Da ein Benutzer mehrere Konten in vielen verschiedenen Profilen besitzen kann, bietet die Benutzersuchfunktion die Möglichkeit, in den nach Besitzernamen sortierten Querverweisen nach Kontodatensätzen zu suchen. Außerdem können Sie in der Benutzersuchfunktion auch Direktaufrufe zum Hinzufügen, Editieren und Löschen bestimmter Kontodatensätze verwenden, ohne den Dialog ’Benutzerprofilmerkmale’ öffnen zu müssen. In den folgenden Abschnitten werden diese Funktionen beschrieben. Sie sollten sich vor allem mit der Suchfunktion vertraut machen, da sie eine Voraussetzung zum Editieren und Löschen von Benutzern ist.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse aufgeführt, die für diese Tasks, die über die Benutzersuchfunktion ausgeführt werden können, erforderlich sind:

Aktivität	Umgebung	Berechtigungsklasse
Einen Benutzerkontodatensatz suchen, editieren oder löschen	Tivoli-Arbeitsoberfläche	**admin**

Voraussetzungen

Bei den hier beschriebenen Vorgängen zur Benutzersuche wird davon ausgegangen, dass Sie folgende Schritte bereits ausgeführt haben:

1. Richtlinienbereich erstellen.
2. Profilmanager erstellen.
3. Ein oder mehrere Benutzerprofile erstellen.
4. Benutzerdatensatz für alle Benutzer erstellen, nach denen Sie suchen, die Sie editieren oder löschen möchten.

Informationen zum Ausführen dieser Schritte finden Sie im *Tivoli Management Framework Benutzerhandbuch* und *Tivoli SecureWay User Administration Management Handbuch* sowie in der Onlinehilfe.

Benutzer hinzufügen

Beim Hinzufügen eines Benutzers wird ein Benutzerkontodatensatz erstellt, der dem von Ihnen angegebenen Benutzerprofil hinzugefügt wird. Der Benutzerkontodatensatz enthält die Informationen, die zum Verwalten des Benutzerkontos erforderlich sind. Diese Benutzerkontoinformationen werden in einer Benutzerprofildatenbank gespeichert und den Systemdateien erst hinzugefügt, wenn Sie das Profil an die Endpunkte verteilen.

So fügen Sie einen Benutzerkontodatensatz unter Verwendung der Benutzersuchfunktion hinzu:

1. Klicken Sie doppelt auf das Symbol der **Benutzersuchfunktion**, das sich auf der Tivoli-Arbeitsoberfläche befindet.

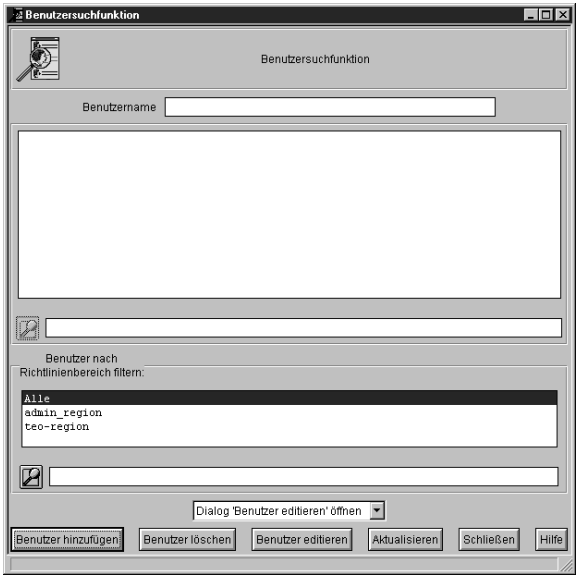
2. Wählen Sie das Profil aus, dem Sie den Benutzer hinzufügen möchten, und klicken Sie auf die Schaltfläche **Hinzufügen**. Daraufhin wird die Anzeige 'Datensatz hinzufügen' aufgerufen.
3. Geben Sie in der Anzeige 'Datensatz hinzufügen' die entsprechenden Daten in den Feldern ein. (Weitere Informationen zur Anzeige 'Datensatz hinzufügen' finden Sie in der Onlinehilfe.)

Benutzer suchen

Wenn Sie mit der Benutzersuchfunktion nach einem bestimmten Benutzernamen suchen, finden Sie alle Kontodatensätze, die dieser Benutzer besitzt. Bei der Suche nach einem Benutzer können Sie die Suche auf einen einzigen Richtlinienbereich eingrenzen oder in der gesamten TMR suchen. Nachdem Sie einen Benutzer gefunden haben, können Sie eine Liste mit den Benutzerprofilen anzeigen, die Datensätze von diesem Benutzer enthalten.

So suchen Sie unter Verwendung der Benutzersuchfunktion nach einem Benutzer:

1. Klicken Sie doppelt auf das Symbol der **Benutzersuchfunktion**, das sich auf der Tivoli-Arbeitsoberfläche befindet.
2. Wählen Sie in der Liste **Benutzer nach Richtlinienbereich filtern** den Richtlinienbereich aus, den Sie durchsuchen möchten. Wenn Sie alle Richtlinienbereiche in der TMR durchsuchen möchten, wählen Sie die Option **Alle** aus.



3. Geben Sie im Feld **Benutzername** eine Zeichenfolge ein, die mit dem Namen des Benutzerdatensatzes übereinstimmt, nach dem Sie suchen, und drücken Sie auf die Eingabetaste. (Dabei muss der Cursor im Feld **Benutzername** aktiv sein.) Die eingegebene Zeichenfolge kann entweder genau dem gesuchten Benutzernamen entsprechen oder auch die unten beschriebenen Platzhalterzeichen enthalten. Daraufhin werden alle Benutzerdatensätze angezeigt, die den Suchkriterien entsprechen.

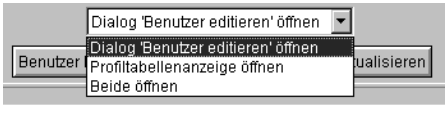
   Anmerkungen:

   a. Bei der Zeichenfolge im Feld ’Benutzername’ wird die Groß-/Kleinschreibung nicht beachtet, d. h., mit den Suchbegriffen “joe smith” bzw. “JOE SMITH” wird beide Male der Benutzername “Joe Smith” gefunden. Sie können den Stern (*) als Platzhalterzeichen für kein, ein oder mehrere unbekannte Zeichen verwenden. Es können auch mehrere Sterne in einem Suchbegriff verwendet werden. So wird z. B. bei Eingabe des Suchbegriffs “j*s*” der Benutzer Joe Smith gefunden.

b. Die beiden Suchfelder, die rechts neben den Lupensymbolen angezeigt werden, ermöglichen eine Suche in dem jeweiligen Fenster, unter dem sie sich befinden. Anders als im Benutzernamensuchfeld werden in diesen Feldern die Übereinstimmungen als reguläre Perl 4-Ausdrücke zurückgegeben. Daher kann das Shell-Platzhalterzeichen (*) nicht angegeben werden, um eine Liste aller Benutzer anzuzeigen. Stattdessen sollte der reguläre Ausdruck Punkt Stern (.*) verwendet werden. Weitere Informationen zu regulären Ausdrücken finden Sie im *Tivoli Management Framework Benutzerhandbuch*.

4. Klicken Sie doppelt auf den hervorgehobenen Benutzernamen, um eine erweiterte Ansicht zu öffnen. Die Einträge in dieser erweiterten Anzeige haben folgendes Format: **Richtlinienbereich;Profilmanager;Profil**.

5. Klicken Sie in der erweiterten Ansicht doppelt auf eine Option, um die Attribute für ein bestimmtes Benutzerkonto zu editieren. Welcher Dialog bzw. welche Dialoge daraufhin angezeigt werden, hängt von der Einstellung in der Dropdown-Liste ab, die sich am unteren Rand des Dialogs 'Benutzersuchfunktion' befindet.



Dialog 'Benutzer editieren' öffnen
Zeigt den Dialog **Datensatz editieren** an. Sie können sofort mit dem Editieren von Attributen für den ausgewählten Benutzer beginnen.

Profiltabellenanzeige öffnen
Zeigt den Dialog **Benutzerprofilmerkmale** an.

Beide öffnen
Zeigt den Dialog **Datensatz editieren** sowie den Dialog **Benutzerprofilmerkmale** an.

Weitere Informationen finden Sie in der Onlinehilfe zu den Anzeigen 'Datensätze editieren' und 'Benutzerprofilmerkmale'.

Benutzer editieren

Sie können die Benutzerdatensätze in den von Ihnen angegebenen Benutzerprofilen editieren. Die geänderten Benutzerkontoinformationen werden in einer Benutzerprofildatenbank gespeichert. Die Änderungen werden erst in die Systemdateien übernommen, wenn Sie das Profil an die Endpunkte verteilen.

So editieren Sie unter Verwendung der Benutzersuchfunktion einen Benutzerkontodatensatz:

1. Klicken Sie doppelt auf das Symbol der **Benutzersuchfunktion**, das sich auf der Tivoli-Arbeitsoberfläche befindet.
2. Suchen Sie nach dem zu ändernden Benutzerdatensatz. Daraufhin werden alle Profile angezeigt, die einen Datensatz für diesen Benutzer enthalten. (Weitere Informationen zur Suche nach Benutzern finden Sie in der Beschreibung der Prozedur „Benutzer suchen" auf Seite 225.)
3. Wählen Sie das Profil aus, in dem Sie den Benutzersatz editieren möchten, und klicken Sie auf die Schaltfläche **Editieren**. Daraufhin wird die Anzeige zum Editieren der Datensätze angezeigt.
4. Geben Sie in dieser Anzeige die entsprechenden Daten in den Feldern ein. (Weitere Informationen hierzu finden Sie in der Onlinehilfe zur Anzeige 'Datensatz editieren'.)

Benutzer löschen

Wenn eine Benutzerdatensatz nicht mehr benötigt wird, können Sie ihn aus dem Benutzerprofil löschen. Wenn Sie das Profil anschließend erneut verteilen, wird der Benutzerdatensatz für Subskribenten gelöscht, die eine neue Programmkopie erhalten.

So löschen Sie einen Benutzerkontodatensatz unter Verwendung der Benutzersuchfunktion:

1. Suchen Sie den zu löschenden Benutzerdatensatz. Daraufhin werden alle Profile angezeigt, die einen Datensatz für diesen Benutzer enthalten. (Weitere Informationen zur Suche nach Benutzern finden Sie in der Beschreibung der Prozedur „Benutzer suchen” auf Seite 225.)
2. Je nachdem, ob der Benutzer sich in nur einem Profil oder in mehreren Profilen befindet, führen Sie einen der folgenden Schritte aus:
   - **Benutzer in nur einem Profil:** Heben Sie entweder den Benutzernamen oder den Profilnamen hervor, und klicken Sie auf die Schaltfläche **Löschen**. Sie werden gefragt, ob Sie das Basisverzeichnis entfernen oder beibehalten oder ob Sie den Vorgang abbrechen möchten. Wählen Sie eine Option aus.
   - **Benutzer in mehreren Profilen:** Wenn Sie den Benutzerdatensatz aus allen Profilen löschen möchten, wählen Sie den Benutzernamen aus, und klicken Sie auf die Schaltfläche **Löschen**. Wenn Sie den Benutzer aus einem bestimmten Profil löschen möchten, wählen Sie das Profil aus, und klicken Sie auf die Schaltfläche **Löschen**. Nachdem Sie auf **Löschen** geklickt haben, werden Sie vom System gefragt, ob Sie das Basisverzeichnis entfernen oder beibehalten oder ob sie den Vorgang abbrechen möchten. Wählen Sie eine Option aus.

Benutzerdatensätze anzeigen

Der Dialog **Benutzerprofilmerkmale** listet jeden Benutzerdatensatz im Profil zeilenweise auf. Jede Spalte enthält spezifische Informationen zum Benutzerdatensatz. Sie können durch dieses Fenster blättern, um die Informationen anzuzeigen, die in einem Benutzerdatensatz gespeichert sind.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklassen, die für diese Task erforderlich sind, aufgeführt:

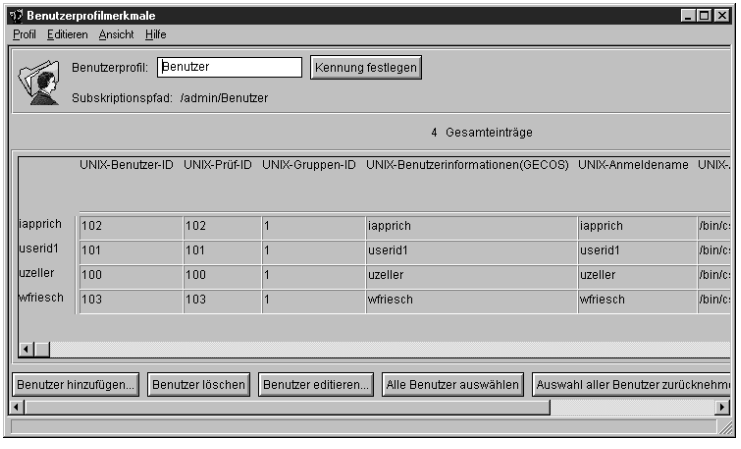
Aktivität	Umgebung	Berechtigungsklassen
Benutzerkontodatensatz anzeigen	Benutzerprofil	**user** **Admin_Add_Account** **Admin_Del_Account** **Admin_Edit_Account** **Admin_Mod_Account** **Admin_View_Account**

Sie können einen Benutzerdatensatz über die Tivoli-Arbeitsoberfläche oder die Befehlszeile anzeigen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um einen Benutzerdatensatz anzuzeigen:

1. Suchen Sie mit dem Dialog **Benutzersuchfunktion** den Benutzer, den Sie anzeigen möchten. Weitere Informationen zur Verwendung der **Benutzersuchfunktion** finden Sie unter „Benutzerdatensätze suchen” auf Seite 223.
2. Öffnen Sie in der Benutzersuchfunktion den Dialog **Benutzerprofilmerkmale** .



3. Ziehen Sie die Schiebeleiste am unteren Rand des Dialogs nach links oder rechts. Durch Ziehen der Schiebeleiste werden die Spalten im Fenster sichtbar.

Befehlszeile

Im folgenden Beispiel werden alle Informationen zum angegebenen Benutzerdatensatz angezeigt:

```
wgetusr @UserProfile:Marketing jtate
```

Dabei gilt Folgendes:

@UserProfile:Marketing
Gibt den Namen des Benutzerprofils an.

jtate Gibt den Anmeldenamen des Benutzers an.

Weitere Informationen hierzu finden Sie in der Beschreibung des Befehls **wgetusr** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Benutzerdatensätze editieren

Wenn Sie den Datensatz eines vorhandenen Benutzerkontos ändern, speichert Tivoli SecureWay User Administration die Benutzerinformationen in einer Benutzerprofildatenbank und sendet einen Hinweis an die Hinweisdatenbank. Die Informationen des Benutzerkontos werden nicht in den Systemdateien oder Systemdatenbanken aktualisiert, es sei denn, Sie verteilen das Profil an seine endgültige Endpunktzieladresse.

Benutzerprofile können während eines Weitergabevorgangs oder einer Verteilung nicht aktualisiert werden. Wenn Sie jedoch einen Datensatz in einem Benutzerprofil über die GUI oder Befehlszeile editieren, wird der Datensatz nicht gesperrt. Wenn Sie Datensätze über die grafische Benutzerschnittstelle (GUI) editieren und den Datensatz festlegen und schließen, um Ihre Änderungen zu speichern, wird der Änderungszeitpunkt für den editierten Datensatz mit dem Änderungszeitpunkt des entsprechenden Datensatzes auf dem Datenträger verglichen. Wenn der bereits gespeicherte Datensatz neuer ist (was bedeutet, dass ein anderer Administrator diesen Datensatz geändert hat, nachdem Sie den Dialog 'Merkmale bearbeiten' aufgerufen haben und bevor Sie versucht haben, Ihre Änderungen zu speichern), erhalten Sie folgende Fehlermeldung:

```
Der von Ihnen editierte Datensatz ist älter als der in der Datenbank
gespeicherte Datensatz. Vor dem Speichern muss der Datensatz erneut
editiert werden. Der Dialog zum Editieren wurde aktualisiert und
zeigt jetzt den neueren Datensatz aus der Datenbank an.
```

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklassen, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklassen
Benutzerkontodatensatz editieren	Benutzerprofil	**admin Admin_Edit_Account Admin_Mod_Account Admin_Mod_Account_LDAP Admin_Mod_Account_NT Admin_Mod_Account_NW Admin_Mod_Account_OS2 Admin_Mod_Account_OS4 Admin_Mod_Account_RF Admin_Mod_Account_UX Admin_Mod_Account_W2K**

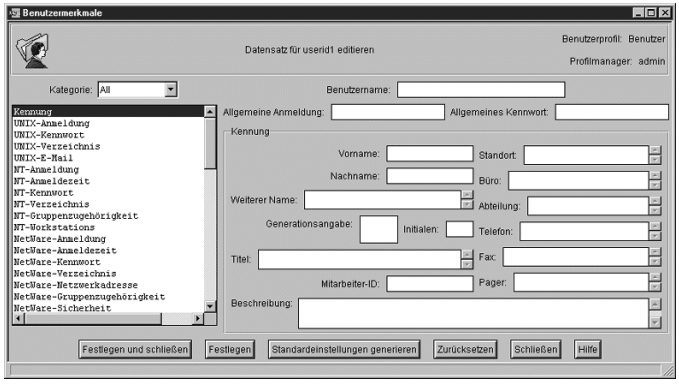
Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um einen Benutzerdatensatz zu editieren:

1. Suchen Sie mit dem Dialog **Benutzersuchfunktion** den Benutzer, den Sie löschen möchten. Weitere Informationen zur Verwendung der **Benutzersuchfunktion** finden Sie unter „Benutzerdatensätze suchen” auf Seite 223.

2. Klicken Sie doppelt auf einen Benutzerdatensatz, um den Dialog **Benutzermerkmale** anzuzeigen.



3. Editieren Sie die Informationen des Benutzerkontos für diesen Benutzerdatensatz.

   Weitere Einzelheiten zur Eingabe von Benutzerinformationen finden Sie unter „Allgemeine Informationen zu Benutzerkonten” auf Seite 160, „Informationen zu Windows NT-Benutzerkonten” auf Seite 172, „Informationen zu NetWare-Benutzerkonten” auf Seite 190 und „Informationen zu UNIX-Benutzerkonten” auf Seite 210.

4. Klicken Sie auf **Festlegen und schließen**, um die Änderungen am Benutzerdatensatz zu speichern und den Dialog zu schließen.

Befehlszeile

Im folgenden Beispiel wird das UNIX-Kennwort des Benutzers geändert:

```
wsetusr –p algebra @UserProfile:marketing "Jon Smith"
```

Dabei gilt Folgendes:

–p algebra
: Gibt an, dass das UNIX-Kennwort des Benutzers in **algebra** geändert wird.

@UserProfile:marketing
: Gibt den Namen des Benutzerprofils an, das den zu ändernden Benutzerdatensatz enthält.

"Jon Smith"
Gibt den wirklichen Namen an, der dem zu ändernden Benutzerdatensatz zugeordnet ist.

Weitere Informationen hierzu finden Sie in der Beschreibung des Befehls **wsetusr** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Benutzerdatensätze zusammenfügen

Mit Tivoli SecureWay User Administration können Sie zwei Benutzerdatensätze, die zu demselben Benutzer gehören, zusammenfügen. Die Benutzerinformationen, die in dem ersten Datensatz gespeichert sind, werden als Hauptdatensatz behandelt. Der zweite Datensatz wird als Quellendatensatz behandelt und selektiv mit dem Hauptdatensatz zusammengefügt. Sobald zwei Datensätze zusammengefügt worden sind, wird der Quellendatensatz aus dem Profil gelöscht.

Während eines Weitergabevorgangs mit dem Befehl **popusers -M** versucht Tivoli SecureWay User Administration ähnliche Benutzerinformationen aus der Füllquelle in die vorhandenen Benutzerdatensätze im Profil einzufügen. Es verwendet den Anmeldenamen als Schlüssel, um zu bestimmen, ob es eine Übereinstimmung gibt.

Wenn die allgemeinen Informationen für die Datensätze zusammengefügt werden, wird das Zusammenfügen auf Attributbasis vorgenommen. Das heißt, dass das Zusammenfügen der allgemeinen Informationen zu einem Mischen von Informationen führen kann. Angenommen, im Hauptdatensatz ist **John** für das Attribut **given name**, **Smith** für das Attribut **last name** und **5359** für das Attribut **telephone** und im Quellendatensatz **Jonathan** für das Attribut **given name**, **Smith** für das Attribut **last name** und **marketing** für das Attribut **department** angegeben. Nach dem Zusammenfügen ist in den allgemeinen Informationen im Hauptdatensatz **John** für das Attribut **given name**, **Smith** für das Attribut **last name**, **marketing** für das Attribut **department** und **5359** für das Attribut **telephone** angegeben.

Wenn die architekturspezifischen Informationen zusammengefügt werden, geschieht dies auf Kontenbasis. Das heißt, wenn beide Datensätze Windows NT-Benutzerinformationen besitzen und der Quellendatensatz über UNIX-Benutzerinformationen verfügt, überschreiben die Windows NT-Benutzerinformationen im Hauptdatensatz die Windows NT-Benutzerinformationen im Quellendatensatz, und die UNIX-Benutzerinformationen aus dem Quellendatensatz werden dem Hauptdatensatz hinzugefügt.

Damit die Zusammensetzung auf dem Endpunkt wirksam wird, muss das Profil verteilt werden.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklassen, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklassen
Zwei Benutzerdatensätze zusammenfügen	Benutzerprofil	**admin** **Admin_Edit_Account**

Sie können diese Task nur über die Befehlszeile ausführen.

Im folgenden Beispiel werden zwei Benutzerdatensätze zusammengefügt:

```
wmrgusrs @UserProfile:marketing jsmith @UserProfile:accounting jon_smith
```

Dabei gilt Folgendes:

@UserProfile:marketing
: Gibt den Namen des Benutzerprofils an, das die zusammenzufügenden Benutzerdatensätze enthält.

jsmith
: Gibt den ersten Benutzerdatensatz an. Tivoli SecureWay User Administration verwendet diesen als Hauptdatensatz.

@UserProfile:accounting
: Gibt den Namen des Benutzerprofils an, das den doppelten Benutzerdatensatz für das Zusammenfügen enthält.

jon_smith
Gibt den zweiten Benutzerdatensatz an. Tivoli SecureWay User Administration verwendet diesen als Quellendatensatz und fügt die Informationen selektiv in den Hauptdatensatz ein.

Weitere Informationen finden Sie in der Beschreibung des Befehls **wmrgusrs** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Benutzerdatensätze löschen

Wenn Sie ein Benutzerkonto nicht mehr benötigen, können Sie es aus dem Profil löschen. Wenn Sie das Profil erneut verteilen, wird der Datensatz aus allen Subskribenten, die die neue Profilkopie erhalten, gelöscht, und das Benutzerkonto wird aus den Konfigurationsdateien des Systems gelöscht.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklassen, die für diese Task erforderlich sind, aufgeführt:

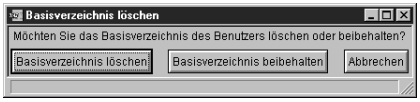
Aktivität	Umgebung	Berechtigungsklassen
Benutzerkontodatensatz löschen	Benutzerprofil	**admin** **Admin_Edit_Account** **Admin_Del_Account**

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um einen Benutzerkontodatensatz zu löschen:

1. Suchen Sie mit dem Dialog **Benutzersuchfunktion** den Benutzer, den Sie löschen möchten. Weitere Informationen zur Verwendung der Benutzersuchfunktion finden Sie unter „Benutzerdatensätze suchen” auf Seite 223.
2. Wählen Sie die zu löschenden Datensätze aus.

3. Klicken Sie auf **Benutzer löschen**, um einen Warndialog anzuzeigen.



Klicken Sie auf **Basisverzeichnis löschen**, um das UNIX-Basisverzeichnis des Benutzers zu löschen, oder klicken Sie auf **Basisverzeichnis beibehalten**, um das UNIX-Basisverzeichnis beizubehalten, das Benutzerkonto bei Verteilung des Profils jedoch zu löschen.

Befehlszeile

Im folgenden Beispiel wird ein Benutzerdatensatz gelöscht:

```
wdelusr -d @UserProfile:sales jtate
```

Dabei gilt Folgendes:

-d Löscht das UNIX-Basisverzeichnis des Benutzers.

@UserProfile:sales
Gibt das Profil an, aus dem der Benutzerdatensatz gelöscht wird.

jtate Gibt den Namen des Benutzerdatensatzes an, der gelöscht wird.

Weitere Informationen finden Sie in der Beschreibung des Befehls **wdelusr** im Handbuch *Tivoli SecureWay User Administration Reference Manual.*

Benutzerdatensätze formatieren

Mit dem Befehl **wusrdbrep** können Sie die Attributwerte aller Benutzerdatensätze innerhalb eines Benutzerprofils formatieren. Hierbei wird eine begrenzte Liste ausgegeben, die in ein Tabellenkalkulationsprogramm oder in eine Datenbankanwendung importiert werden kann.

Anmerkung: Mit dem Befehl **wusrdbrep** können Sie die Attributwerte zwar auch anzeigen, die Ausgabe ist jedoch für den Import in ein Tabellenkalkulationsprogramm oder

in eine Datenbankanwendung bestimmt. Zum Anzeigen von Attributen sollten Sie den Befehl **wgetusr** verwenden.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Benutzerdatensätze formatieren	Benutzerprofil	**super**

Diese Option ist nur über die Befehlszeile verfügbar.

Im folgenden Beispiel werden die Attributwerte der Benutzerdatensätze eines Benutzerprofils aufgelistet:

```
wusrdbrep -f salesvalues @UserProfile:sales
```

Dabei gilt Folgendes:

-f salesvalues
Gibt die Ausgabedatei mit der begrenzten Liste an. Wird kein absoluter Pfad angegeben, wird die Ausgabedatei im aktuellen Verzeichnis gespeichert. Wird die Option **-f** nicht angegeben, wird die Ausgabe an den Bildschirm gesendet.

@UserProfile:sales
Gibt das Profil an, dessen Werte aufgelistet werden sollen.

Weitere Informationen finden Sie in der Beschreibung des Befehls **wusrdbrep** im Handbuch *Tivoli SecureWay User Administration Reference Manual.*

Ausgabe des Befehls 'wusrdbrep'

Bei der Ausgabe des Befehls **wusrdbrep** handelt es sich um eine begrenzte Liste, die in ein Tabellenkalkulationsprogramm oder in eine Datenbankanwendung importiert werden kann. Aus der ersten Zeile der Liste gehen die Attribute des Benutzerdatensatzes hervor. In den folgenden Zeilen werden für jeden Benutzerdatensatz des angegebenen Profils die Werte der einzelnen Attribute aufgeführt.

Es folgt ein verkürztes Beispiel für die Ausgabe des Befehls **wusrdbrep**. Die tatsächliche Ausgabe ist vom jeweiligen Profil abhängig und enthält in der Regel eine weit höhere Anzahl Attribute und Werte.

Security_Groups,**add_new_subscribers**,audit_flag,audit_id, city,comment,department,employee_id,entry_flags,fax,fixed, gcos,gen_qual-,gid,given_name,group_aliases,hd_contents, hd_local_path,hd_server-_path,hd_type,initials,**key**, last_name,**location**,...

″″,**ENABLED**,0,126,,″<David is responsible for project D.>
<He works from both Austin and Chicago.>″,″<887j>″,
″89643″,458760,″<999-9999>,DISABLED,″Dave″,″Mr″,″1″,
″David″,, ″denmor:\etc\Tivoli\Tivoli_Admin\hd_contents″,
″/home/daved″,″denmor:/export/home/daved″,1,″D″,
″**1149013884.1.652_0**″,″Dever″,″**<Austin, TX 78727>**″,...

″″,**ENABLED**,0,127,,″<This is the description for Sue.>
<No special notes made.>″,″<776y>″,″76543″,458760,″<898-8989>″,DISABLED,″Sue″,″Ms″,″1″,″Susan″,,″denmor:\etc\Tivoli\Tivoli_Admin\hd_contents″,″/home/sues″,
″denmor:/export/home/sues″,1,″s″,″**1149013884.1.652_1**″,
″Shobuck″,″**<Austin, Tx 78727>**″,...

Dieses Beispiel enthält Ausschnitte aus zwei Benutzerdatensätzen. In beiden Benutzerdatensätzen ist das Attribut **add_new_subscribers** aktiviert. Für **location** gilt Austin, Texas, mit dem Postzustellbezirk 78727. Der erste Benutzerdatensatz verfügt jedoch über den **Schlüssel** 1149013884.1.652_0, der **Schlüssel** des zweiten Benutzerdatensatzes lautet 1149013884.1.652_1.

Die Formatierung der Attributwerte in der Ausgabeliste folgt folgender Struktur:

- Zeichenfolgen werden in Anführungszeichen gesetzt. Der Attributwert `Horace` wird z. B. folgendermaßen formatiert: `"Horace"`.

  Enthält eine Zeichenfolge Anführungszeichen, werden diese in der formatierten Liste verdoppelt. So wird zum Beispiel die

Zeichenfolge `Owner of the "smart" brand` folgendermaßen formatiert: `"Owner of the ""smart"" brand"`.

Enthält eine Zeichenfolge einen Ausdruck in eckigen Klammern, werden diese in der formatierten Liste verdoppelt. Die Zeichenfolge `Department 12<bldg1>` z. B. wird folgendermaßen formatiert: `"Department 12<<bldg1>>"`.

Ein Zeilenumbruch oder ein Rücklaufzeichen innerhalb einer Zeichenfolge wird durch eine Leerstelle dargestellt.

Leere Zeichenfolgen werden folgendermaßen formatiert: `""`.

- Bei Zeichenfolgenlisten handelt es sich um Attribute, die über mehr als einen Wert verfügen und aus mindestens einer Zeichenfolge bestehen. Die Zeichenfolgenlisten werden in der Ausgabeliste in Anführungszeichen gesetzt. Die einzelnen Zeichenfolgenelemente, aus der sich die Zeichenfolgenliste zusammensetzt, werden in folgende Zeichen gesetzt: <>.

  Die Zeichenfolgenliste

  ```
  Machine A   Machine B   Machine C
  ```

  wird z. B. folgendermaßen formatiert:

  ```
  "<Machine A><Machine B><Machine C>"
  ```

  Anführungszeichen und eckige Klammern innerhalb einer Zeichenfolgenliste werden in der formatierten Liste verdoppelt (wie auch bei einfachen Zeichenfolgen).

- Numerische Werte werden nicht in Anführungszeichen gesetzt. Der Attributwert `304` wird z. B. folgendermaßen formatiert: `304`.
- Boolesche Werte werden in der formatierten Liste entweder als `ENABLED` oder als `DISABLED` angezeigt.
- Kennwörter werden wie folgt dargestellt: `"***"`.
- Die Attribute **nw_acct_exp_date**, **nw_pass_date_expires** und **nt_expiredate** werden folgendermaßen formatiert: `"MM/TT/YYYY HH:MM"`.
- Oktettlisten werden als Listen mit hexadezimalen Werten formatiert. Der Oktettwert `00000001 11111100 11100000` wird z. B. folgendermaßen formatiert: `X'01FCE0'`.

- Wurde einem Attribut ein einem Benutzerdatensatz kein Wert zugeordnet, enthält die Ausgabeliste an dieser Stelle ein Komma (**,**).

Weitere Informationen zu Attributen und Werten von Benutzerprofilen können Sie dem Handbuch *Tivoli SecureWay User Administration Reference Manual* entnehmen.

Benutzerdatensätze aus Tivoli entfernen

Wenn Sie ein Benutzerkonto nicht länger mit Tivoli SecureWay User Administration verwalten wollen, dieses Konto jedoch nicht aus den Konfigurationsdateien des Systems löschen möchten, können Sie die Option -r des Befehls **wdelusr** verwenden. Diese Option ist nur über die Befehlszeile verfügbar. Im folgenden Beispiel wird ein Benutzerdatensatz entfernt:

```
wdelusr -r @UserProfile:sales jtate
```

Dabei gilt Folgendes:

-r Leitet einen rekursiven Löschvorgang ein. Der Benutzer wird sofort aus der Tivoli-Datenbank entfernt, ohne verteilt zu werden. Das Benutzerkonto wird jedoch auf den Systemen, auf denen es sich gegenwärtig befindet, belassen. Dieses Benutzerkonto wird außerdem nicht mehr von Tivoli verwaltet.

@UserProfile:sales
Gibt das Profil an, aus dem der Benutzerdatensatz gelöscht wird.

jtate Gibt den Namen des Benutzerdatensatzes an, der gelöscht wird.

Weitere Informationen finden Sie in der Beschreibung des Befehls **wdelusr** im Handbuch *Tivoli SecureWay User Administration Reference Manual.*

Gruppenprofile an Subskribenten verteilen

Nachdem Sie ein Benutzerprofil erstellt und diesem Datensätze hinzugefügt bzw. Benutzerdatensätze editiert haben, können Sie das Pro-

fil an die Subskribenten verteilen. Es gibt zwei Subskriptionsebenen für Tivoli SecureWay User Administration:

- Die Option **Profilmanagersubskribenten** legt die Endpunkte und Profilmanager fest, an die der Inhalt des Profils von Tivoli SecureWay User Administration verteilt wird.
- Bei Auswahl der Option **Subskribenten auf Datensatzebene** wird überprüft, an welche Untergruppe dieser Endpunkte oder Profilmanager die einzelnen Datensätze verteilt werden.

Die Profilmanagersubskribenten umfassen zum Beispiel die Endpunkte **tejas**, **fuji** und **mckinley**. Das Profil enthält fünf Datensätze. Die Subskribenten für den ersten Datensatz sind **tejas** und **mckinley**. Der Subskribent für den zweiten Datensatz ist **fuji**. Die Subskribenten für den dritten Datensatz sind **tejas** und **fuji**. Die Subskribenten für den vierten Datensatz sind **tejas** und **mckinley**. Die Subskribenten für den letzten Datensatz sind **tejas**, **fuji** und **mckinley**. Alle Datensätze werden an alle Subskribenten verteilt. Ergebnis der Verteilung dieses Profils:

- Die Datensätze 1, 3, 4 und 5 werden an den Endpunkt **tejas** verteilt.
- Die Datensätze 2, 3 und 5 werden an den Endpunkt **fuji** verteilt.
- Die Datensätze 1, 4 und 5 werden an den Endpunkt **mckinley** verteilt.

Informationen zum Zuordnen von Tivoli-Ressourcen als Subskribenten zu einem Profilmanager finden Sie im *Tivoli Management Framework Benutzerhandbuch*.

Anmerkung: Bevor Sie ein Benutzerprofil an einen NetWare-Endpunkt verteilen, müssen Sie zunächst den Befehl **wsetnds** ausführen. Mit diesem Befehl können Sie auf die NetWare-NDS-Baumstruktur zugreifen. Weitere Informationen finden Sie im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

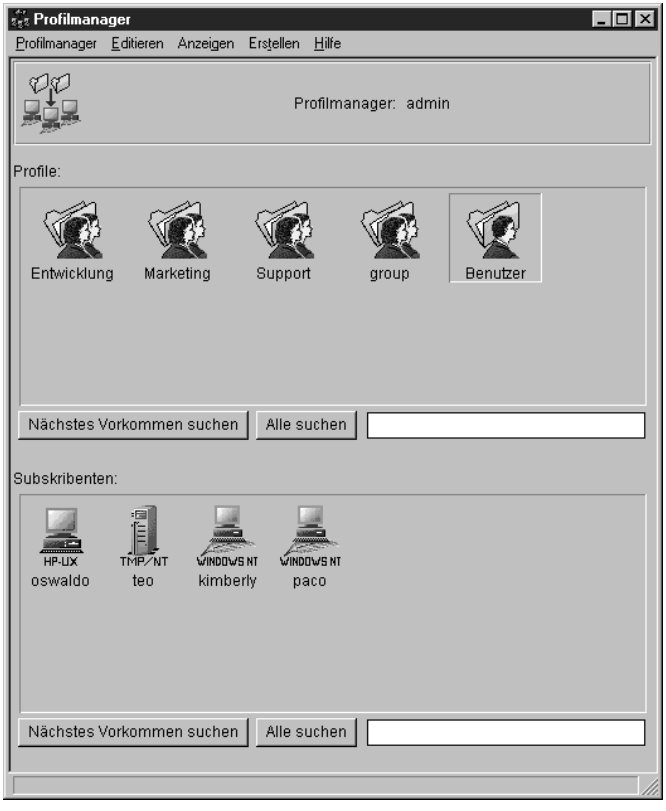
Aktivität	Umgebung	Berechtigungsklasse
Benutzerprofile verteilen	Richtlinienbereich von Subskribenten	**admin**

Sie können ein Benutzerprofil von der Originalkopie oder der Subskriptionskopie eines Profils oder über die Befehlszeile verteilen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Benutzerprofile an Subskribenten von einem Profil aus zu verteilen:

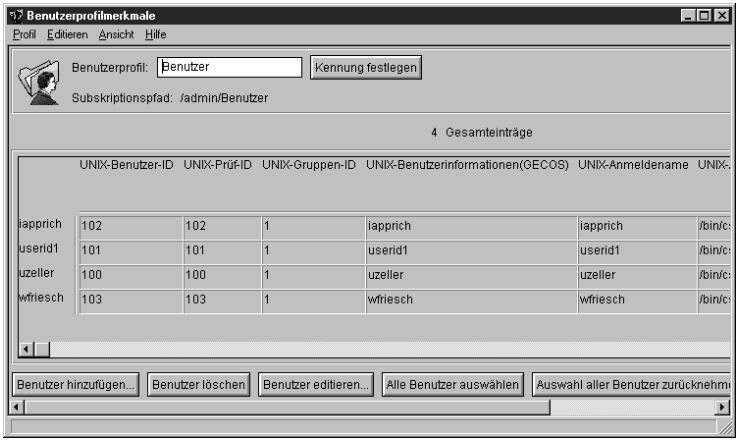
1. Klicken Sie doppelt auf das Symbol des Profilmanagers, um das Fenster **Profilmanager** anzuzeigen.



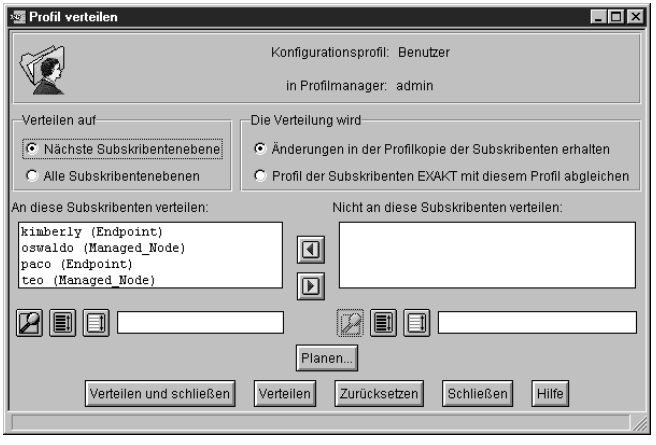
2. Fügen Sie dem Profilmanager die erforderlichen Subskribenten hinzu.

   Weitere Informationen zum Zuordnen von Ressourcen als Subskribenten zu einem Profilmanager finden Sie im *Tivoli Management Framework Benutzerhandbuch.*

3. Klicken Sie doppelt auf das Symbol eines Benutzerprofils, um das Fenster **Benutzerprofilmerkmale** anzuzeigen.



4. Wählen Sie die Option **Verteilen** im Menü **Profil** aus (wenn die Option **Verteilen** inaktiv ist, sichern Sie das Profil, und versuchen Sie es erneut), um den Dialog **Profil verteilen** anzuzeigen.



5. Klicken Sie auf **Nächste Subskribentenebene** im Feld **Verteilen auf**, um eine Kopie des Profils nur an die nächste Subskribentenebene zu senden. Verwenden Sie diese Option, wenn Sie die Kopien der Subskribenten nicht auf allen unteren Ebenen in der Subskriptionshierarchie ändern möchten.

   Anmerkung: Wenn die nächste Ebene der Subskribenten die Ebene des verwalteten Knotens ist, wird das Profil nur an den Tivoli-verwalteten Knoten verteilt und nicht an die eigentlichen Systemdateien. Zum Ändern der Systemdateien mit dieser Option müssen Sie das Profil von der Ebene des verwalteten Knotens verteilen.

   — ODER —

   Klicken Sie auf das Optionsfeld **Alle Subskribentenebenen**, um eine Kopie des Profils an die nächste Ebene von Subskribenten und deren Subskribenten zu senden. Verwenden Sie diese Option, wenn Sie die Subskribenten auf allen unteren Ebenen in der Subskriptionshierarchie und sogar die eigentlichen Systemdateien der Profilendpunkte ändern möchten.

6. Klicken Sie auf **Änderungen in der Profilkopie des Subskribenten erhalten** im Feld **Die Verteilung wird**, um Änderungen beizubehalten, die Administratoren an den Profilen vorgenommen haben, deren Profilmanager dem aktuellen Profil zugeordnet sind. Benutzen Sie diese Option, wenn Profile in Subskribenten definiert wurden, deren Unterschiede Sie beibehalten möchten.

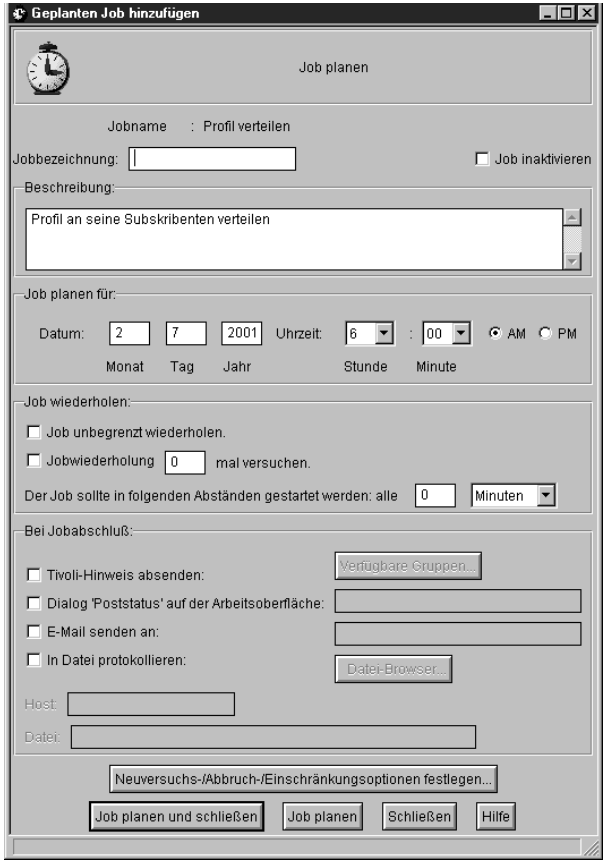
   — ODER —

   Klicken Sie auf **Profil der Subskribenten EXAKT mit diesem Profil abgleichen**, um die Änderungen, die Administratoren an den Profilen vorgenommen haben, mit den in diesem Profil definierten Werten zu überschreiben. Benutzen Sie diese Option, wenn Sie die Unterschiede zwischen den Profilen der Subskribenten nicht beibehalten möchten. Detaillierte Informationen zu den möglichen direkten Folgen dieser Option finden Sie unter Weitere Themen.

7. Wählen Sie in der Liste **Nicht an diese Subskribenten verteilen** die Subskribenten aus, an die Kopien dieses Profils verteilt werden sollen.
8. Klicken Sie auf den Linkspfeil, um die ausgewählten Subskribenten in die Liste **An diese Subskribenten verteilen** zu verschieben.
9. Klicken Sie auf **Verteilen und schließen**, um das Profil sofort zu verteilen und zum Dialog **Benutzerprofilmerkmale** zurückzukehren.

   — ODER —

   Klicken Sie auf **Planen**, um den Dialog **Geplanten Job hinzufügen** anzuzeigen.



Sie können mit diesem Dialog das Verteilen von Profilen für einen späteren Zeitpunkt planen oder Tivoli SecureWay User Administration ermöglichen, eine fehlgeschlagene Verteilung erneut zu versuchen, bis sie erfolgreich ist oder einen konfigurierbaren Wiederholungszähler erreicht. Einzelheiten zur Verwendung der Tivoli-Planungsfunktion finden Sie im *Tivoli Management Framework Benutzerhandbuch*.

Befehlszeile

Im folgenden Beispiel wird ein Benutzerprofil an einen zugeordneten verwalteten Knoten verteilt:

```
wdistrib -l maintain -m @UserProfile:development \
@ManagedNode:rushmore
```

Dabei gilt Folgendes:

-l maintain
Behält alle lokalen Änderungen in den Subskribentenkopien des Profils bei.

-m Gibt eine Verteilung in mehreren Schritten an. Das Profil wird an alle Ebenen der Subskribenten verteilt, einschließlich der Systemdateien.

@UserProfile:development
Gibt den Namen des Profils an, das verteilt werden soll.

@ManagedNode:rushmore
Gibt den Namen des Subskribenten an, an den das Profil verteilt wird.

Weitere Informationen zur Verteilung von Benutzerprofilinformationen und zu deren Planung finden Sie in der Beschreibung der Befehle **wdistrib** und **wschedjob** im Handbuch *Tivoli Framework Reference Manual*.

Benutzerdatensätze verwalten

Nachdem Sie die erforderlichen Basisvorgänge zum Definieren und Verteilen von Benutzerprofilen ausgeführt haben, müssen Sie möglicherweise einige Vorgänge zur Datenpflege ausführen, um sicherzustellen, dass die in einem Benutzerprofil enthaltenen Informationen auf dem aktuellen Stand bleiben.

Führen Sie die folgenden Prozeduren durch, um Ihre Benutzerdatensätze zu verwalten:

- Benutzerdatensätze kopieren
- Benutzerdatensätze verschieben
- Informationen in Benutzerdatensätzen sperren und freigeben
- Das Fenster ″Benutzerprofilmerkmale″ aktualisieren
- Benutzerdatensätze mit der Tivoli-Datenbank synchronisieren
- Benutzerdatensätze überprüfen
- Benutzerdatensätze abrufen
- Benutzerdatensätze suchen
- Von einer Profilkopie in eine andere wechseln
- Benutzerdatensätze sortieren
- Benutzerdatensatzattribute sortieren

Benutzerdatensätze kopieren

Durch das Kopieren von Benutzerdatensätzen aus einem Profil in ein anderes wird eine exakte Kopie der Benutzerkontodatensätze aus dem Quellenprofil in dem vorhandenen Zielprofil erstellt.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklassen, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklassen
Benutzerdatensätze zwischen Benutzerprofilen kopieren	Benutzerprofil	**admin** **Admin_Edit_Account** **Admin_Add_Account**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte durch, um Benutzerdatensätze zu kopieren:

1. Suchen Sie mit dem Dialog **Benutzersuchfunktion** den Benutzer, den Sie kopieren möchten. Weitere Informationen zur Verwendung der **Benutzersuchfunktion** finden Sie unter „Benutzerdatensätze suchen” auf Seite 223.
2. Wählen Sie den zu kopierenden Datensatz aus.
3. Wählen Sie **Benutzer kopieren** im Menü **Editieren** aus, um den Dialog **Profildatensätze kopieren** anzuzeigen.

In der Liste **Verfügbare Profilmanager** werden die Profilmanager angezeigt, in denen die Profile enthalten sind, in die die ausgewählten Datensätze kopiert werden können.

4. Wählen Sie den Profilmanager, der die zu kopierenden Profildatensätze enthält, in der Liste **Verfügbare Profilmanager** aus.
5. Wählen Sie in der Liste **Verfügbare Profile** die Profile aus, in die die Datensätze kopiert werden sollen. Klicken Sie auf den Rechtspfeil, um die Profile in die Liste **Zielprofile** zu verschieben.
6. Klicken Sie auf **Kopieren und schließen**, um die Datensätze in die Zielprofile zu kopieren und den Dialog zu schließen.

   Tivoli SecureWay User Administration fügt die Datensätze den angegebenen Profilen hinzu.

Befehlszeile

Im folgenden Beispiel wird ein Benutzerdatensatz aus einem Profil in ein anderes kopiert:

```
wcpusr @UserProfile:region_1 @UserProfile:sales_1 jtate
```

Dabei gilt Folgendes:

@UserProfile:region_1
: Gibt den Namen des Profils an, aus dem der Benutzerdatensatz kopiert wird.

@UserProfile:bsales_1
: Gibt den Namen des Profils an, in das der Benutzerdatensatz kopiert wird.

jtate
: Gibt den Anmeldenamen des zu kopierenden Benutzerdatensatzes an.

Weitere Informationen hierzu finden Sie in der Beschreibung des Befehls **wcpusr** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Benutzerdatensätze verschieben

Mit Tivoli SecureWay User Administration können Sie Datensätze aus einem Benutzerprofil in ein anderes verschieben.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklassen, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklassen
Benutzerkontodatensatz verschieben	Benutzerprofil	**admin** **Admin_Edit_Account**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Benutzerdatensätze zu verschieben:

1. Suchen Sie mit dem Dialog **Benutzersuchfunktion** den Benutzer, den Sie verschieben möchten. Weitere Informationen zur Verwendung der **Benutzersuchfunktion** finden Sie unter „Benutzerdatensätze suchen” auf Seite 223.
2. Wählen Sie die zu verschiebenden Datensätze aus.
3. Wählen Sie **Datensätze verschieben** im Menü **Editieren** aus, um den Dialog **Datensätze verschieben** (früher: Datensätze versetzen) anzuzeigen.

4. Wählen Sie den Profilmanager, der das Zielprofil enthält, in der Liste **Verfügbare Profilmanager** aus. Tivoli SecureWay User Administration zeigt alle für diesen Profilmanager verfügbaren Profile in der Liste **Verfügbare Profile** an.
5. Wählen Sie das Zielprofil in der Liste **Verfügbare Profile** aus.
6. Klicken Sie auf **Verschieben und schließen** (früher: Versetzen und schließen), um den ausgewählten Benutzerkontodatensatz in das Zielprofil zu verschieben und zum Dialog **Benutzerprofilmerkmale** zurückzukehren.

Befehlszeile

Im folgenden Beispiel wird ein Benutzerdatensatz aus einem Profil in ein anderes verschoben:

```
wmvusr @UserProfile:region_1 @UserProfile:region_4 lmiles
```

@UserProfile:region_1
Gibt das Quellenbenutzerprofil an.

@UserProfile:region_4
Gibt das Zielbenutzerprofil an.

lmiles Gibt den Anmeldenamen an, der dem zu verschiebenden Benutzerdatensatz zugeordnet ist.

Weitere Informationen hierzu finden Sie in der Beschreibung des Befehls **wmvusr** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Informationen in Benutzerdatensätzen sperren und freigeben

Durch Sperren der Informationen in einem Benutzerdatensatz wird verhindert, dass Administratoren diesen Datensatz in einer Kopie des Profils editieren oder löschen. Sie müssen das Benutzerprofil verteilen, damit die Sperre wirksam wird. Die Subskribenten können einen Datensatz so lange weder bearbeiten noch löschen, bis Sie diesen freigeben und das Profil erneut verteilen.

Sie können alle Datensätze in einem Profil der höchsten Ebene sperren, um sicherzustellen, dass seine Kopien stets unverändert bleiben. Da Sie nicht das gesamte Profil sperren können, kann ein Administrator einen Datensatz der Kopie eines Profils der unteren Ebene hinzufügen.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklassen, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklassen
Benutzerkontodatensatz sperren oder freigeben	Benutzerprofil	**admin** **Admin_Edit_Account** **Admin_Mod_Account**

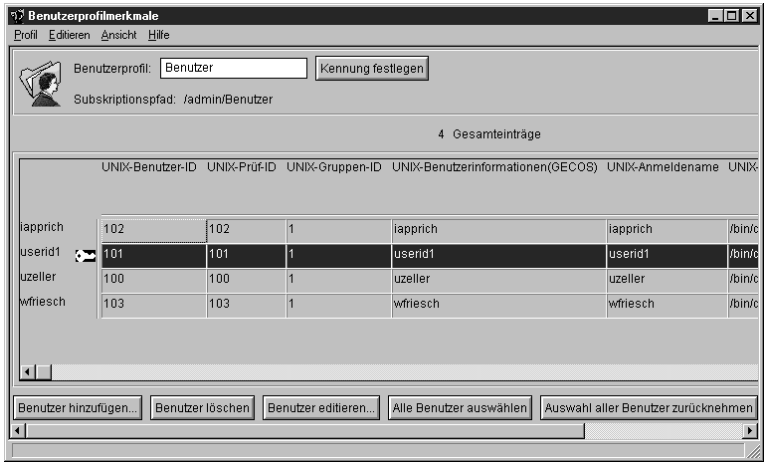
Sie können einen Benutzerdatensatz über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile sperren.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um einen Benutzerdatensatz zu sperren oder freizugeben:

1. Suchen Sie mit dem Dialog **Benutzersuchfunktion** den Benutzer, den Sie sperren oder freigeben möchten.

2. Wählen Sie den zu sperrenden oder freizugebenden Benutzerdatensatz aus.
3. Öffnen Sie in der Benutzersuchfunktion den Dialog **Benutzerprofilmerkmale**.
4. Wählen Sie die Option **Datensätze sperren** im Menü **Editieren** aus. Tivoli SecureWay User Administration platziert eine Schlüsselglyphe neben den Datensatz, um anzuzeigen, dass dieser gesperrt ist.



5. Wählen Sie zum Freigeben eines Datensatzes einen gesperrten Datensatz und dann die Option **Datensätze freigeben** im Menü **Editieren** aus. Tivoli SecureWay User Administration entfernt die Schlüsselglyphe.

Befehlszeile

Im folgenden Beispiel wird ein Benutzerdatensatz gesperrt:

```
wsetusr –F @UserProfile:marketing jtate
```

Dabei gilt Folgendes:

–F Gibt an, dass die Subskribenten die Kopie des Benutzerdatensatzes nach der nächsten Profilverteilung nicht ändern können.

@UserProfile:marketing
Gibt den Namen des Benutzerprofils an, das den Datensatz enthält.

jtate Gibt den Anmeldenamen des Benutzers an.

Weitere Informationen hierzu finden Sie in der Beschreibung des Befehls **wsetusr** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Das Fenster ″Benutzerprofilmerkmale″ aktualisieren

Wenn andere Administratoren berechtigt sind, im selben Benutzerprofil wie Sie Benutzerkontodatensätze hinzuzufügen, zu editieren oder zu löschen, dann müssen Sie möglicherweise das Fenster **Benutzerprofilmerkmale** aktualisieren. Das Fenster **Benutzerprofilmerkmale** zeigt den Inhalt des Profils zum Zeitpunkt seiner Öffnung bzw. der letzten Aktualisierung an. Daher können Sie das Ergebnis der Aktionen anderer Administratoren im Profil erst sehen, nachdem Sie das Fenster **Benutzerprofilmerkmale** entweder geschlossen und erneut geöffnet oder es aktualisiert haben.

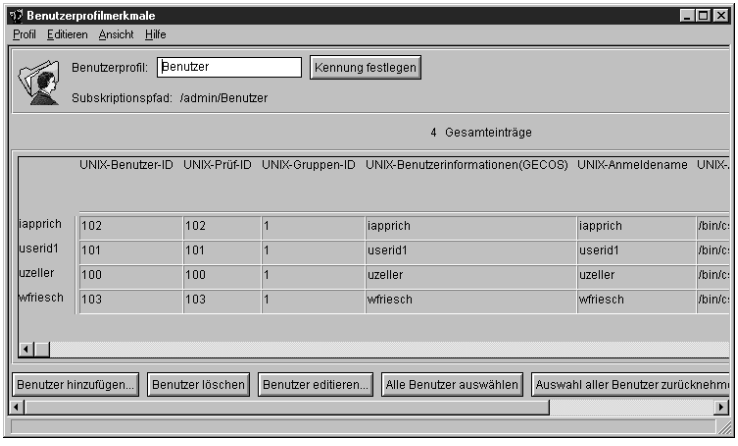
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Fenster **Benutzerprofilmerkmale** aktualisieren	Benutzerprofil	**user**

Sie können diese Task nur über die Tivoli-Arbeitsoberfläche ausführen.

Führen Sie folgende Schritte aus, um das Fenster **Benutzerprofilmerkmale** zu aktualisieren:

1. Klicken Sie doppelt auf ein Benutzerprofil, um das Fenster **Benutzerprofilmerkmale** anzuzeigen.



2. Wählen Sie **Aktualisieren** im Menü **Profil** aus, um das Fenster **Benutzerprofilmerkmale** zu aktualisieren.

Benutzerdatensätze mit der Tivoli-Datenbank synchronisieren

Wenn die Systemkonfigurationsdateien direkt editiert werden, stimmt das Profil nicht mehr mit den Systemdateien überein, für die es die Informationen bereitstellt. Das Synchronisieren des Profils und seiner zugehörigen Datenbank mit Systemdateien zeigt Ihnen, welche Datensätze nicht mit den Einträgen in der Systemdatei übereinstimmen. Anschließend wird Ihnen aufgezeigt, wie Sie das Profil mit der Systemdatei abgleichen können.

Die Synchronisationsfunktion von Tivoli SecureWay User Administration synchronisiert nicht die Benutzerkennwörter, da diese normalerweise vom Benutzer verwaltet werden.

Anmerkung: Sie können die PC-Endpunkte (Windows NT-Domänen oder NetWare-NDS-Baumstrukturen) nur über die Befehlszeile synchronisieren.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

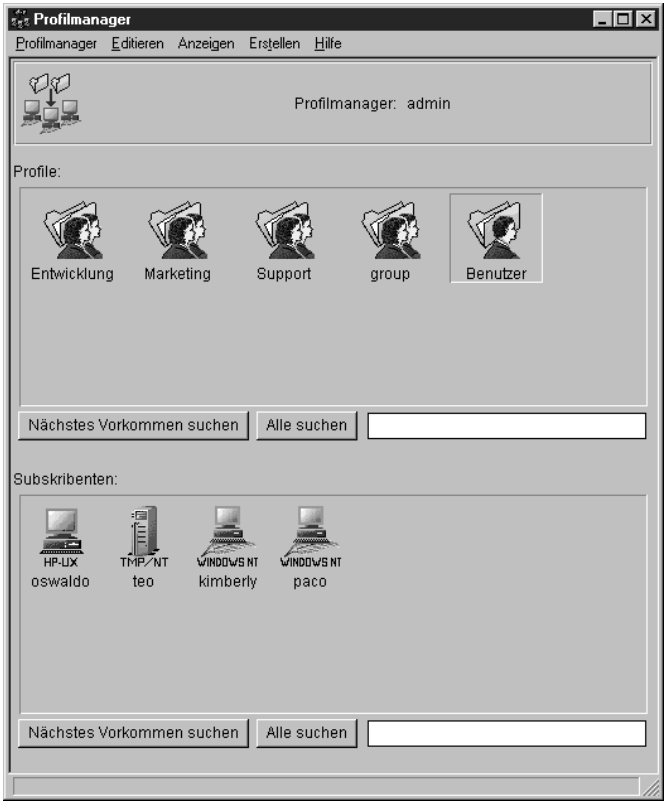
Aktivität	Umgebung	Berechtigungsklasse
Profildatenbank mit Systemdateien synchronisieren	Benutzerprofil	**admin**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um die Profildatenbank mit Systemdateien zu synchronisieren:

1. Klicken Sie doppelt auf das Symbol des Profilmanagers, um das Fenster **Profilmanager** anzuzeigen.



2. Wählen Sie den Subskribenten aus, mit dem Sie die Benutzerprofile synchronisieren möchten.
3. Wählen Sie **Synchronisieren** im Kontextmenü des ausgewählten Subskribenten aus, um den Dialog **Profile synchronisieren** anzuzeigen.

4. Wählen Sie die Profilart **UserProfile** in der Liste **Verfügbare Profilarten** aus.
5. Klicken Sie auf **Synchronisieren**, um die Profildatenbank mit dem Subskribentensystem zu überprüfen.

   Tivoli überprüft das Profil und die Subskribentensysteme auf Unterschiede, anschließend zeigt es den Dialog **Profil-/Systemdiskrepanzen** an.

   Der Dialog **Profil-/Systemdiskrepanzen** zeigt die Unterschiede zwischen den Benutzerkonfigurationsdateien auf den Subskribentensystemen und dem aktuellen Profil an. Sie können auf **Änderungen festschreiben** klicken, um die Informationen aus den Systemdateien in das Profil zu kopieren. Sie können aber auch auf **Schließen** klicken und die erforderlichen Änderungen vornehmen, indem Sie dem Profil Einträge manuell hinzufügen oder Einträge manuell daraus löschen.

Anmerkung: Mit einer Synchronisation wird nur die Kopie des Profils des verwalteten Knotens aktualisiert, nicht das Profil der höchsten Ebene.

Befehlszeile

Sie können den Befehl **wchkusrs** verwenden, um die Benutzerdatensätze in einer Systemdatei mit den Benutzerdatensätzen in einem Benutzerprofil zu vergleichen. Wenn Sie Benutzerdatensätze vergleichen, gibt der Befehl **wchkusrs** eine Liste mit Benutzerdatensätzen zurück, die sich in der Systemdatei und nicht im Benutzerprofil befinden, und eine Liste mit Benutzerdatensätzen, die sich in beiden befinden, jedoch unterschiedlich sind. Beispiel:

```
wchkusrs @UserProfile:nbUSER01 @ManagedNode:puma
```

Dabei gilt Folgendes:

@UserProfile:nbUSER01
Gibt den Namen des zu überprüfenden Profils an.

@ManagedNode:puma
Gibt den Namen des Systems an, anhand dessen die Überprüfung erfolgt.

Dieser Befehl gibt Informationen nach dem folgenden Muster zurück:

```
Endpunkt
@ManagedNode:puma wird geprüft...

Diese Benutzer wurden zwar im System, nicht aber im
angegebenen Profil bzw. in der angegebenen Datenbank gefunden:

Root   smtp
listen
nancy
joe
sweetp

Diese Benutzer wurden im angegebenen Profil bzw. in der angegebenen
Datenbank, aber nicht im System gefunden:

jon03
robyn
bbranden

Diese Unterschiede wurden im Profil bzw. in der Datenbank nicht aktualisiert. Verwenden Sie zur Aktualisierung den Befehl wchkusrs mit Option -f.
```

Weitere Informationen hierzu finden Sie in der Beschreibung des Befehls **wchkusrs** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Benutzerdatensätze überprüfen

Tivoli SecureWay User Administration überprüft automatisch Datensätze anhand der Profilrichtlinie, wenn ein Datensatz hinzugefügt oder geändert wird. Tivoli SecureWay User Administration überprüft allerdings nur die Attribute von Benutzerdatensätzen, die der Richtlinie für Gültigkeitsprüfung zugeordnet wurden. Wenn die Richtlinie für Gültigkeitsprüfung geändert wurde, seit Sie das letzte Mal Datensätze hinzugefügt oder geändert haben, können Sie alle Datensätze des Profils auf einmal überprüfen, um so die Datensätze zu finden, die der neuen Richtlinie nicht entsprechen.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Datensätze in Bezug auf die Profilrichtlinien überprüfen	Benutzerprofil	**admin**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Führen Sie folgende Schritte aus, um Datensätze nach Änderung der Richtlinie anhand der Profilrichtlinie zu überprüfen:

1. Suchen Sie mit dem Dialog **Benutzersuchfunktion** den Benutzer, den Sie überprüfen möchten. Weitere Informationen zur Verwendung der **Benutzersuchfunktion** finden Sie unter „Benutzerdatensätze suchen” auf Seite 223.
2. Öffnen Sie in der Benutzersuchfunktion den Dialog **Benutzerprofilmerkmale**.
3. Wählen Sie die zu überprüfenden Datensätze aus.
4. Wählen Sie **Auswerten** im Menü **Profil** aus, das sich im Fenster **Benutzerprofilmerkmale** befindet, um den Dialog **Ergebnisse der Richtliniengültigkeitsprüfung** anzuzeigen, in dem die Datensätze aufgelistet werden, die die Gültigkeitsprüfung nicht bestanden haben.

Benutzerdatensätze abrufen

Sie können eine neue Kopie eines Profils aus dem Profilmanager abrufen, der sich in der Subskriptionshierarchie eine Ebene höher befindet. Dieser Vorgang ist im Kern eine Anfrage an den zugeordneten Profilmanager auf Verteilung an einen einzelnen Subskribenten. Sie können eine neue Subskriptionskopie nur innerhalb eines Subskribenten abrufen.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

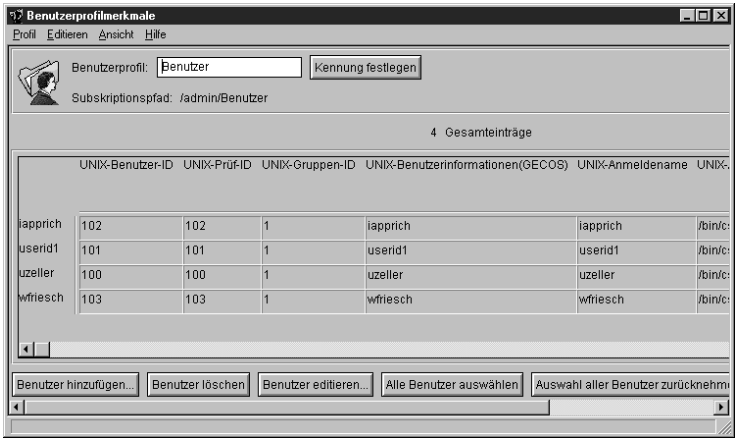
Aktivität	Umgebung	Berechtigungsklasse
Benutzerprofilkopien aus einem anderen Profilmanager abrufen	Benutzerprofil zuordnen	**admin**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

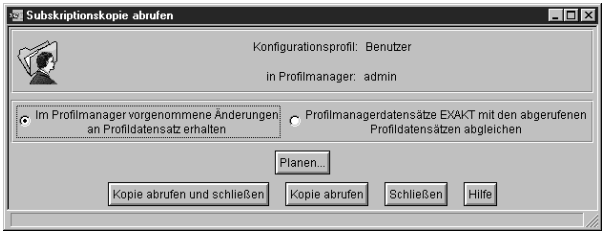
Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Benutzerprofilkopien aus einem anderen Profilmanager abzurufen:

1. Klicken Sie doppelt auf das Symbol eines Benutzerprofils, um das Fenster **Benutzerprofilmerkmale** anzuzeigen.



2. Wählen Sie **Neue Kopie abrufen** im Menü **Profil** aus, um den Dialog **Subskriptionskopie abrufen** anzuzeigen.

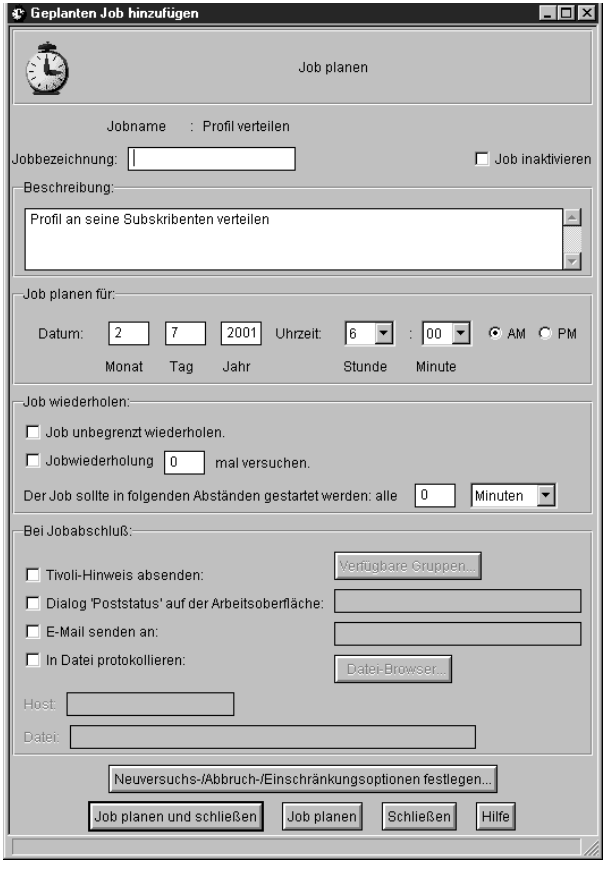


3. Klicken Sie auf **Profilmanagerdatensätze EXAKT mit den abgerufenen Profildatensätzen abgleichen**, um das Profil abzurufen und die Werte im aktuellen Profil zu überschreiben. Verwenden Sie diese Option, wenn Sie die lokalen Änderungen an Ihrem aktuellen Profil nicht beibehalten möchten.

   — ODER —

Klicken Sie auf **Im Profilmanager vorgenommene Änderungen an Profildatensatz erhalten**, um das Profil abzurufen und die Werte im aktuellen Profil beizubehalten. Verwenden Sie diese Option, wenn Sie die Einstellungen in Ihrem Profil nach dem Abrufen des neuen Profils beibehalten möchten.

4. Damit Sie das Profil zu einem späteren Zeitpunkt abrufen können, klicken Sie auf **Planen**, um den Dialog **Geplanten Job hinzufügen** anzuzeigen.



Sie können mit diesem Dialog das Verteilen von Profilen für einen späteren Zeitpunkt planen oder Tivoli SecureWay User Administration ermöglichen, eine fehlgeschlagene Verteilung erneut zu versuchen, bis sie erfolgreich ist oder einen konfigurierbaren Wiederholungszähler erreicht. Einzelheiten zur Verwendung der Tivoli-Planungsfunktion finden Sie im *Tivoli Management Framework Benutzerhandbuch*.

5. Klicken Sie auf **Kopie abrufen und schließen**, um sofort Kopien der Profildatensätze im aktuellen Profil zu erhalten und den Dialog zu schließen.

Befehlszeile

Im folgenden Beispiel wird die Kopie eines Profils aus einem anderen Profilmanager abgerufen:

```
wgetprf -l maintain @ProfileManager:design
```

Dabei gilt Folgendes:

- l maintain Behält alle lokalen Änderungen in den Subskribentenkopien des Profils bei.

@ProfileManager:BluesModem
Gibt den Namen des Subskribenten an, für den die neue Profilkopie abgerufen wird.

Weitere Informationen zum Abrufen von Benutzerprofilinformationen aus einem anderen Profil mit Hilfe der Befehlszeile finden Sie in der Beschreibung des Befehls **wgetprf** im Handbuch in the *Tivoli Framework Reference Manual*.

Benutzerdatensätze suchen

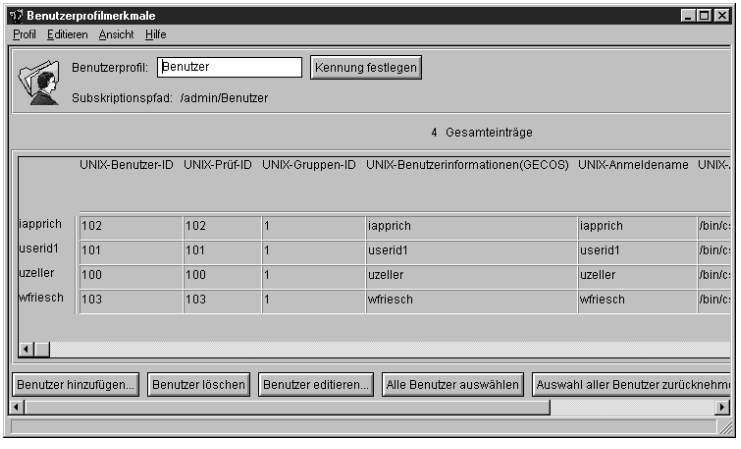
Tivoli SecureWay User Administration stellt Ihnen den Dialog **Benutzersuchfunktion** zum Suchen von Benutzern (ohne ein Profil zu öffnen) bereit. Es gibt jedoch Situationen, in denen Sie ein Profil geöffnet haben und dort einen Benutzer suchen müssen. Tivoli SecureWay User Administration stellt Ihnen ein Tool für die Suche nach Benutzern in einem Profil zur Verfügung.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

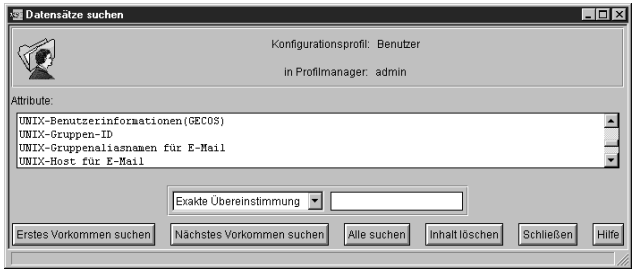
Aktivität	Umgebung	Berechtigungsklasse
Benutzerdatensatz in einem Benutzerprofil suchen	Benutzerprofil	**user**

Sie können diese Task nur über die Tivoli-Arbeitsoberfläche ausführen. Führen Sie folgende Schritte aus, um einen Benutzerdatensatz in einem Benutzerprofil zu suchen:

1. Klicken Sie im Profilmanager doppelt auf ein Profil, um das Fenster **Benutzerprofilmerkmale** anzuzeigen.



2. Wählen Sie **Suchen** im Menü **Ansicht** aus, um den Dialog **Datensätze suchen** anzuzeigen.



3. Wählen Sie die entsprechenden Attribute in der Liste **Attribute** aus. Diese Attribute werden von Tivoli SecureWay User Administration zur Definition der Suchkriterien verwendet.

4. Wählen Sie eine der folgenden Sucharten aus dem Kontextmenü aus:

   - **Enthält**

     Gibt an, dass die gefundenen Datensätze den Wert des Suchbegriffs enthalten.

   - **Exakte Übereinstimmung**

     Gibt an, dass die gefundenen Datensätze mit dem Suchbegriff exakt übereinstimmen.

   - **Größer als**

     Gibt an, dass der Wert des ausgewählten Attributs für die gefundenen Datensätze größer ist als der Wert des Suchbegriffs.

   - **Kleiner als**

     Gibt an, dass der Wert des ausgewählten Attributs für die gefundenen Datensätze kleiner ist als der Wert des Suchbegriffs.

5. Geben Sie einen Wert für den Suchbegriff ein. Der Suchbegriff für das Attribut kann ein beliebiger gültiger Wert sein.
6. Klicken Sie auf **Erstes Vorkommen suchen**, um das erste Vorkommen eines lokalen Druckdienstes zu suchen, das mit dem Suchbegriff übereinstimmt.

   — ODER —

   Klicken Sie auf **Nächstes Vorkommen suchen**, um das nächste Vorkommen eines lokalen Druckdienstes zu suchen, das mit dem Suchbegriff übereinstimmt.

   — ODER —

   Klicken Sie auf **Alle suchen**, um alle lokalen Druckdienste zu suchen, die mit dem Suchbegriff übereinstimmen.

Von einer Profilkopie in eine andere wechseln

Sie können von einem beliebigen Profil zu einer anderen Kopie des aktuellen Profils in der Subskriptionshierarchie wechseln und diese anzeigen. Abhängig von Ihrer Berechtigungsklasse können Sie für die neu angezeigte Profilkopie Vorgänge ausführen.

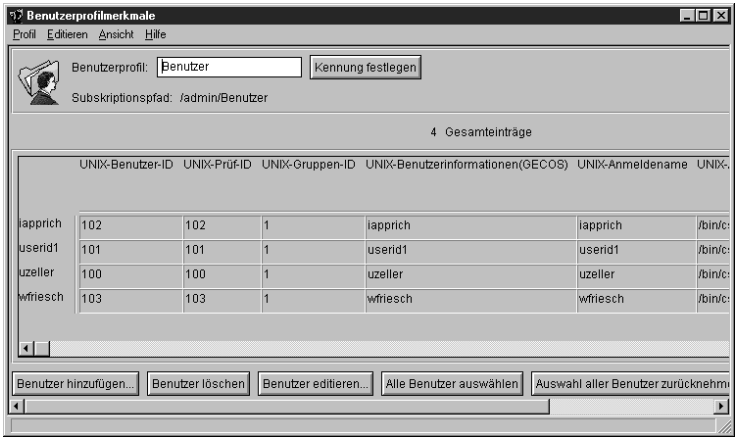
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Von einer Profilkopie in eine andere wechseln	Benutzerprofil	**user**

Sie können diese Task nur über die Tivoli-Arbeitsoberfläche ausführen.

Führen Sie folgende Schritte aus, um zwischen Benutzerprofilkopien zu wechseln:

1. Klicken Sie im Profilmanager doppelt auf ein Profil, um das Fenster **Benutzerprofilmerkmale** anzuzeigen.



2. Wählen Sie **Zu Profil auf** im Menü **Profil** aus, um den Dialog **Zu Profil** anzuzeigen.

3. Wählen Sie den Subskribenten mit der Kopie des anzuzeigenden Profils aus.
4. Wählen Sie die Kopie des anzuzeigenden Profils aus.
5. Klicken Sie auf **Zu Profil...**, um die Profilkopie anzuzeigen oder zu editieren.

Benutzerdatensätze sortieren

Sie können die Reihenfolge festlegen, in der die Benutzerkontodatensätze im Fenster **Benutzerprofilmerkmale** angezeigt werden. Wenn Sie jedoch das Fenster schließen, geht die Sortierung verloren. Wenn Sie das Fenster erneut öffnen, werden die Datensätze in der Standardreihenfolge angezeigt.

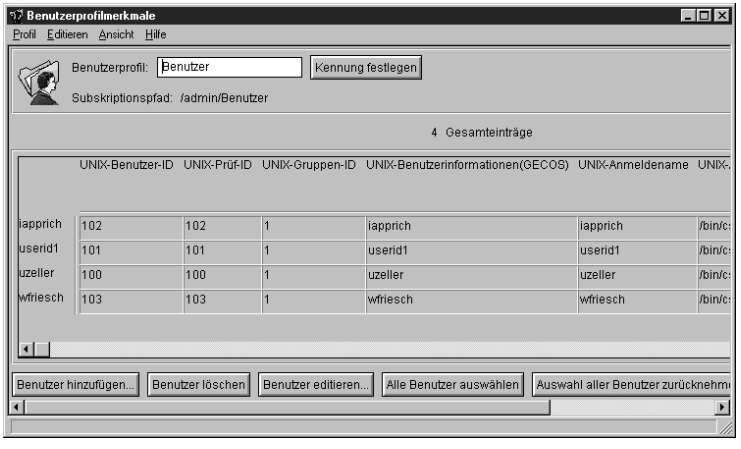
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Benutzerdatensätze sortieren	Benutzerprofil	**user**

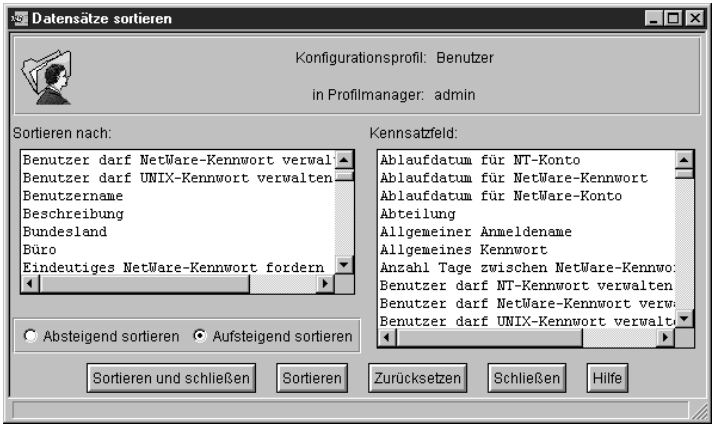
Sie können diese Task nur über die Tivoli-Arbeitsoberfläche ausführen.

Führen Sie folgende Schritte aus, um Benutzerdatensätze zu sortieren:

1. Klicken Sie im Profilmanager doppelt auf ein Profil, um das Fenster **Benutzerprofilmerkmale** anzuzeigen.



2. Wählen Sie im Menü **Ansicht** nacheinander **Sortieren –> Benutzer** aus, um den Dialog **Datensätze sortieren** anzuzeigen.



3. Wählen Sie in der Liste **Sortieren nach** das Attribut aus, nach dem sortiert werden soll. Die Datensätze in dem Profil werden dann nach dem von Ihnen ausgewählten Attribut sortiert.

4. Wählen Sie ein Attribut aus, dessen Kennung in der linken Spalte des Fensters **Benutzerprofilmerkmale** angezeigt werden soll. Sie können in der linken Spalte des Profilfensters die linke Maustaste drücken, um Datensätze auszuwählen.

5. Klicken Sie auf **Sortieren und schließen**, um die Datensätze zu sortieren und zum Fenster **Benutzerprofilmerkmale** zurückzukehren.

Benutzerdatensatzattribute sortieren

Sie können festlegen, welche Benutzerattribute angezeigt und in welcher Reihenfolge diese im Fenster **Benutzerprofilmerkmale** aufgeführt werden. Wenn Sie jedoch das Fenster schließen, geht die Sortierung verloren. Wenn Sie das Fenster erneut öffnen, werden die Datensätze in der Standardreihenfolge angezeigt.

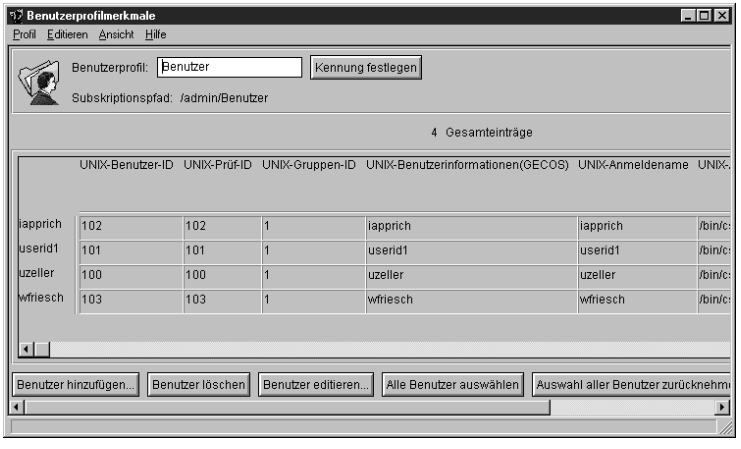
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Datensatzattribute sortieren und anzeigen	Benutzerprofil	**user**

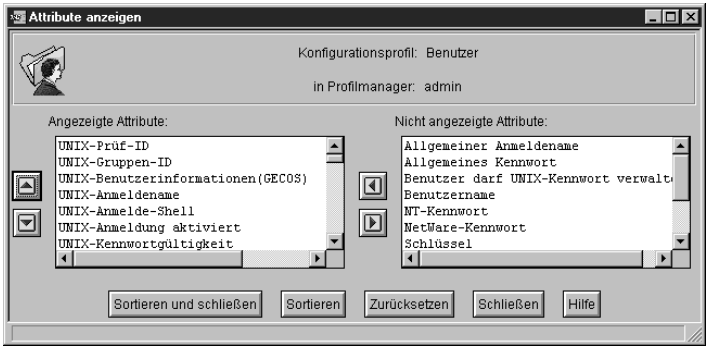
Sie können diese Task nur über die Tivoli-Arbeitsoberfläche ausführen.

Führen Sie folgende Schritte aus, um die Benutzerattribute zu sortieren:

1. Klicken Sie im Profilmanager doppelt auf ein Profil, um das Fenster **Benutzerprofilmerkmale** anzuzeigen.



2. Wählen Sie im Menü **Ansicht** nacheinander **Sortieren –> Attribute** aus, um das Fenster **Attribute anzeigen** anzuzeigen.



3. Wählen Sie die Attribute aus, die in der Liste **Angezeigte Attribute** nicht angezeigt werden sollen. Klicken Sie auf den Rechtspfeil, um das ausgewählte Attribut in die Liste **Nicht angezeigte Attribute** zu verschieben.

4. Wählen Sie ein Attribut in der Liste **Angezeigte Attribute** aus, und klicken Sie auf den Aufwärtspfeil oder den Abwärtspfeil, um es an die Position zu verschieben, an der es im Fenster **Benutzerprofilmerkmale** angezeigt werden soll.

   Wiederholen Sie diesen Schritt, bis alle Attribute in der gewünschten Reihenfolge aufgelistet werden.

5. Klicken Sie auf **Sortieren und schließen**, um die Attribute zu sortieren und anzuzeigen und dann zum Fenster **Benutzerprofilmerkmale** zurückzukehren.

8

Gruppenprofile einrichten

In diesem Kapitel wird das Einrichten von Gruppenprofilen erläutert. Folgende Tasks werden beschrieben:

- Gruppenprofile als verwaltete Ressourcen zuordnen
- Gruppenprofil erstellen
- Gruppenprofil klonen
- Gruppenprofil löschen
- Standardwertegruppe definieren
- Richtlinie für Gültigkeitsprüfung definieren
- Daten an ein Gruppenprofil weitergeben
- Standardwerte für die Verteilung setzen

Mit Gruppenprofilen arbeiten

Ein Gruppendatensatz enthält die erforderlichen Informationen über eine Gruppe. Ein Gruppenprofil ist eine Gruppe von Gruppendatensätzen. Jedes Gruppenprofil enthält eine Reihe von Standardwertegruppen und Richtlinien für Gültigkeitsprüfung. Standardwertegruppen definieren Standardwerte, die verwendet werden, wenn Sie einen neuen Profildatensatz erstellen. Richtlinien für Gültigkeitsprüfung definieren zulässige Werte für die Optionen in einem Profildatensatz.

Anmerkungen:

1. Tivoli SecureWay User Administration verwaltet nur UNIX-Gruppen von Gruppenprofilen in UNIX-verwalteten Knoten und Endpunkten oder in NIS-Domänen.
2. In Gruppenprofilen kommen Sperren auf Profilebene zur Anwendung, keine Sperren auf Datensatzebene. Es kann jeweils nur ein Administrator Änderungen an einem Gruppenprofil vornehmen.

Gruppenprofile als verwaltete Ressourcen zuordnen

Jeder Richtlinienbereich unterhält eine Liste mit verwalteten Ressourcenarten, die für den spezifischen Richtlinienbereich gültig sind oder definiert wurden. Sie müssen Gruppenprofile als verwaltete Ressourcen hinzufügen, bevor Sie einen Richtlinienbereich für die Verwaltung von Gruppen verwenden können. Standardwertegruppen definieren Standardwerte, die verwendet werden, wenn Sie einen neuen Profildatensatz erstellen. Richtlinien für Gültigkeitsprüfung definieren zulässige Werte für die Optionen in einem Profildatensatz.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungs-klasse
Gruppenprofile als verwaltete Ressourcen für einen Richtlinienbereich hinzufügen	Richtlinienbereich	**senior**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Gruppenprofile als verwaltete Ressourcen für den Richtlinienbereich hinzuzufügen:

1. Wählen Sie in der Liste **Verfügbare Ressourcen** die Option **GroupProfile** aus, und klicken Sie auf den Linkspfeil. Dadurch wird die ausgewählte verwaltete Ressource in die Liste **Aktuelle Ressourcen** verschoben.

2. Klicken Sie auf **Festlegen und schließen**, um die neue verwaltete Ressource dem Richtlinienbereich hinzuzufügen und den Dialog zu schließen.

Befehlszeile

Im folgenden Beispiel werden dem Richtlinienbereich Gruppenprofile als verwaltete Ressourcen hinzugefügt:

```
wsetpr GroupProfile @ProfileManager:Noon-region
```

Dabei gilt Folgendes:

GroupProfile
: Gibt die verwaltete Ressourcenart an, die dem Richtlinienbereich hinzugefügt werden soll.

@ProfileManager:Noon-region
: Gibt den Namen des Richtlinienbereichs an.

Weitere Informationen zum Hinzufügen von Gruppenprofilen als verwaltete Ressourcen für einen Richtlinienbereich mit Hilfe der Befehlszeile finden Sie in der Beschreibung des Befehls **wsetpr** im Handbuch *Tivoli Framework Reference Manual*.

Gruppenprofile erstellen

Zum Verwalten von Gruppenkonten mit Tivoli SecureWay User Administration müssen Sie zuerst ein Gruppenprofil erstellen. Profile werden in Profilmanagern erstellt. Zunächst ist das Profil leer, d. h., es enthält keine Datensätze. Es enthält jedoch eine Reihe von Standardwertegruppen und Richtlinien für Gültigkeitsprüfung, die von Tivoli bereitgestellt werden. Sie können diese Gruppen und Richtlinien verwenden oder Ihre eigenen definieren. Standardwertegruppen und Richtlinien für Gültigkeitsprüfung werden in den Gruppenprofilen definiert.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

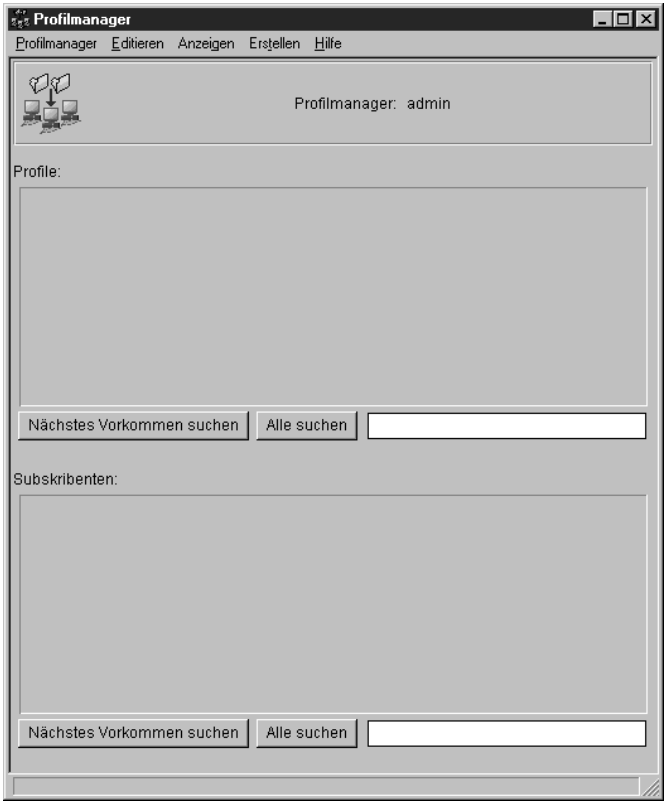
Aktivität	Umgebung	Berechtigungsklasse
Gruppenprofil erstellen	Profilmanager	**senior**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um ein Gruppenprofil zu erstellen:

1. Klicken Sie im Richtlinienbereich doppelt auf das Symbol eines Profilmanagers, um das Fenster **Profilmanager** anzuzeigen.



2. Wählen Sie im Menü **Erstellen** die Option **Profil** aus, um den Dialog **Profil erstellen** anzuzeigen.

Anmerkung: Profile, die sich in demselben Richtlinienbereich befinden, dürfen nicht denselben Namen haben, selbst wenn sie in unterschiedlichen Profilmanagern erstellt werden.

3. Geben Sie einen eindeutigen Name für das Profil im Feld **Name/Symbolbezeichnung** ein.
4. Wählen Sie **GroupProfile** in der Liste **Art** aus.
5. Klicken Sie auf **Erstellen und schließen**, um das Profil zu erstellen und zum Fenster **Profilmanager** zurückzukehren.

   Tivoli erstellt das Gruppenprofil und zeigt im Fenster **Profilmanager** das Symbol des Profils an.

Befehlszeile

Im folgenden Beispiel wird ein neues Gruppenprofil erstellt:

```
wcrtprf @PolicyRegion:UNIX_groups GroupProfile \
developers
```

Dabei gilt Folgendes:

@PolicyRegion:UNIX_groups
: Gibt den Namen des Profilmanagers an, in dem das Gruppenprofil erstellt werden soll.

GroupProfile
: Gibt die zu erstellende Profilart an.

developers
: Gibt den Namen des neuen Gruppenprofils an.

Informationen zum Erstellen eines Gruppenprofils über die Befehlszeile finden Sie in der Beschreibung des Befehls **wcrtprf** im Handbuch *Tivoli Framework Reference Guide*.

Gruppenprofile klonen

Durch das Klonen eines Gruppenprofils wird eine exakte Kopie eines vorhandenen Profils erstellt, einschließlich seiner Standardwertegruppen und Richtlinien, aber ohne seine Datensätze. Zwei Profile derselben Art in demselben Profilmanager können nicht dieselben Datensätze enthalten.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

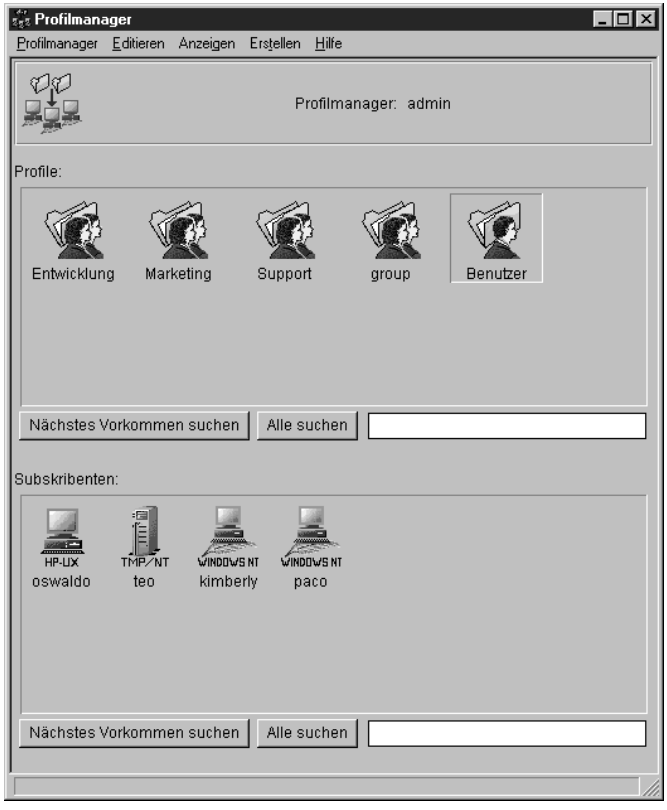
Aktivität	Umgebung	Berechtigungsklasse
Benutzerprofil klonen	Profilmanager	**senior**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um ein Gruppenprofil zu klonen:

1. Klicken Sie in einem Richtlinienbereich doppelt auf das Symbol eines Profilmanagers, um das Fenster **Profilmanager** anzuzeigen.



2. Wählen Sie das Symbol des zu klonenden Profils aus.

3. Wählen Sie im Menü **Editieren** die Optionen **Profile –> Klonen** aus, um den Dialog **Profil klonen** anzuzeigen.

4. Geben Sie den Namen des neuen Profils im Feld **Name/Symbolbezeichnung** ein.
5. Klicken Sie auf **Klonen und schließen**, um das neue Profil zu erstellen und zum Fenster **Profilmanager** zurückzukehren.

   Tivoli erstellt das neue Profil mit allen Standardwertegruppen und Richtlinien des geklonten Profils.

Befehlszeile

Im folgenden Beispiel wird ein Gruppenprofil geklont:

```
wcrtprf -c @GroupProfile:developers \
@ProfileManager:UNIX_groups GroupProfile testers
```

Dabei gilt Folgendes:

-c @GroupProfile:developers
: Gibt den Namen des Profils an, das geklont werden soll.

@ProfileManager:UNIX_groups
: Gibt den Namen des Profilmanagers an, in dem das neue Profil erstellt werden soll.

GroupProfile
Gibt die zu erstellende Profilart an.

testers
Gibt den Namen des neuen Gruppenprofils an.

Informationen zum Klonen eines Gruppenprofils über die Befehlszeile finden Sie in der Beschreibung des Befehls **wcrtprf** im Handbuch *Tivoli Framework Reference Guide*.

Gruppenprofile löschen

Durch Löschen eines Gruppenprofils werden das ursprüngliche Profil und seine Datensätze sowie Kopien aus den Subskribenten des Profilmanagers gelöscht. Durch das Löschen eines Gruppenprofils werden jedoch keine Gruppen-Benutzerinformationen aus den Konfigurationsdateien der Subskribentensysteme gelöscht. Um den Inhalt der Konfigurationsdateien des Systems zu löschen, müssen Sie alle Datensätze des Profils löschen und das Profil anschließend an den Profilendpunkt verteilen. Dadurch wird alles gelöscht, mit Ausnahme der Option **root** und der NIS-Anweisungen in der Konfigurationsdatei.

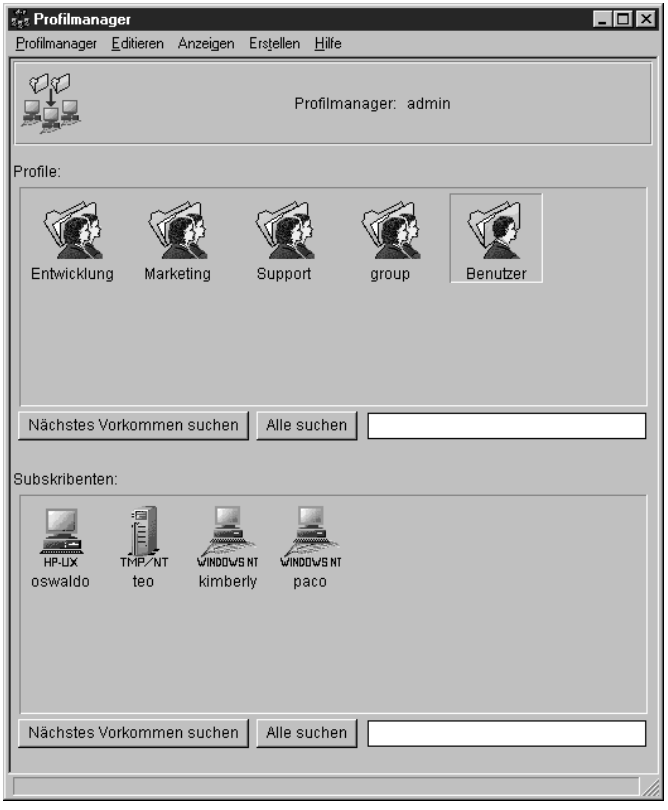
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Gruppenprofil löschen	Profilmanager	**senior**

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um ein Gruppenprofil zu löschen:

1. Klicken Sie in einem Richtlinienbereich doppelt auf das Symbol eines Profilmanagers, um das Fenster **Profilmanager** anzuzeigen.



2. Wählen Sie ein zu löschendes Profil aus.

3. Wählen Sie im Menü **Editieren** die Optionen **Profile –> Löschen** aus, um einen Bestätigungsdialog anzuzeigen.

4. Klicken Sie auf **Löschen**, um das Profil zu löschen und zum Fenster **Profilmanager** zurückzukehren.

Befehlszeile

Im folgenden Beispiel wird ein Gruppenprofil gelöscht:

```
wdel @GroupProfile:marketing
```

Dabei gilt Folgendes:

@GroupProfile:marketing
Gibt das zu löschende Gruppenprofil an.

Informationen zum Löschen eines Gruppenprofils über die Befehlszeile finden Sie in der Beschreibung des Befehls **wdel** im Handbuch *Tivoli Framework Reference Manual*.

Mit Richtlinien von Gruppenprofilen arbeiten

Jedes Benutzerprofil enthält eine Reihe von Standardwertegruppen und Richtlinien für Gültigkeitsprüfung. Standardwertegruppen definieren Standardwerte, die verwendet werden, wenn Sie einen neuen Profildatensatz erstellen. Richtlinien für Gültigkeitsprüfung legen die zulässigen Werte für die Optionen von Profildatensätzen fest.

Standardwertegruppen definieren

Die Standardwertegruppen des Profils geben die Standardwerte an, die verwendet werden, wenn ein neuer Datensatz hinzugefügt wird. Standardwertegruppen sind profilspezifisch.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

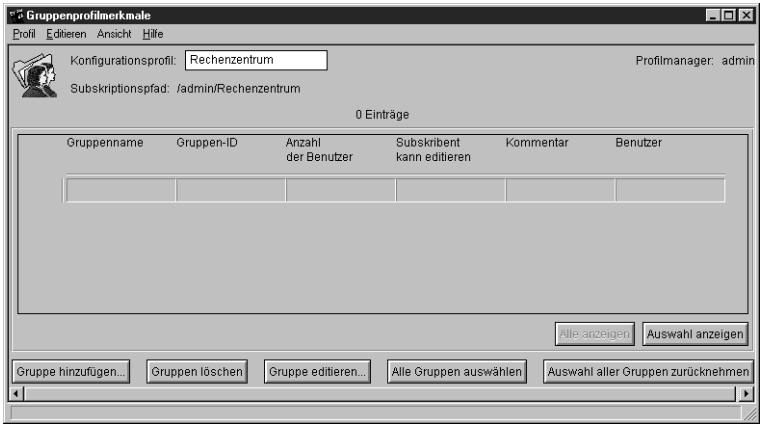
Aktivität	Umgebung	Berechtigungsklasse
Standardwertegruppen von Gruppenprofilen editieren	Gruppenprofil	**senior**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Standardwertegruppen von Gruppenprofilen zu editieren:

1. Klicken Sie in einem Profilmanager doppelt auf das Symbol eines Gruppenprofils, um das Fenster **Gruppenprofilmerkmale** anzuzeigen.



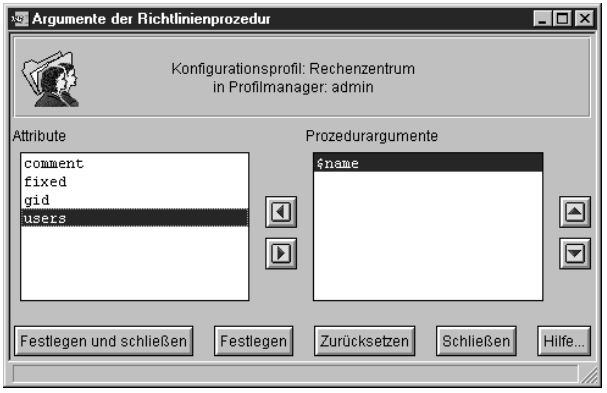
2. Wählen Sie **Standardwertegruppen** im Menü **Editieren** aus, um den Dialog **Standardwertegruppen editieren** anzuzeigen.

3. Wählen Sie ein Attribut in der Liste **Attribute** aus.
4. Klicken Sie auf das Optionsfeld **Ja** im Feld **Subskribenten können Richtlinie editieren**, damit Subskribenten Änderungen durchführen können. Klicken Sie andernfalls auf das Optionsfeld **Nein**.
5. Wählen Sie eine Standardart in der Dropdown-Liste **Standardart** aus. Die verfügbaren Optionen lauten: **Keine**, **Konstante** oder **Skript** (früher: Prozedur).

   Wenn Sie die Option **Konstante** auswählen, geben Sie einen konstanten Wert in das Feld **Wert** ein.

   Führen Sie folgende Schritte aus, wenn Sie die Option **Skript** ausgewählt haben:

   a. Klicken Sie auf **Skriptargumente editieren** (früher: Prozedurargumente editieren), um den Dialog **Argumente des Richtlinienskripts** (früher: Argumente der Richtlinienprozedur) anzuzeigen. Bestimmen Sie mit diesem Dialog die Reihenfolge der Skriptargumente.

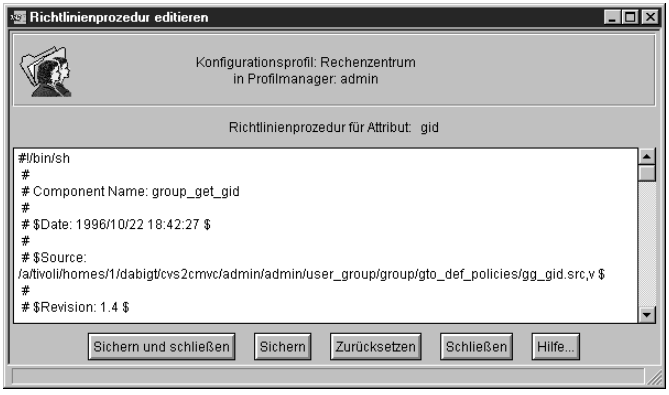


b. Wählen Sie die Datensatzattribute, die die Skriptargumente für das Richtlinienskript des aktuellen Attributs werden sollen, in der Liste **Attribute** aus. Klicken Sie auf den Rechtspfeil, um die Attribute in die Liste **Skriptargumente** (früher: Prozedurargumente) zu verschieben.

   Sie können die Reihenfolge ändern, in der ein Argument aufgerufen wird, indem Sie das Argument auswählen und auf den Aufwärtspfeil bzw. den Abwärtspfeil klicken, um das Argument an die gewünschte Position zu verschieben.

c. Klicken Sie auf **Festlegen und schließen**, um die neuen Argumente hinzuzufügen und zum Dialog **Standardwertegruppen editieren** zurückzukehren.

d. Klicken Sie im Dialog **Standardwertegruppen editieren** auf **Skripthauptteil editieren** (Prozedurhauptteil editieren), um den Dialog **Richtlinienskript editieren** (Richtlinienprozedur editieren) anzuzeigen.



e. Geben Sie den Hauptteil des Skripts ein.

f. Klicken Sie auf **Speichern und schließen** (früher: Sichern und schließen), um das Skript in der Datenbank zu speichern und zum Dialog **Standardwertegruppen editieren** zurückzukehren.

   Wiederholen Sie diesen Vorgang für jedes Attribut des Datensatzes.

6. Klicken Sie auf **Festlegen und schließen**, um die Änderungen anzuwenden und zum Fenster **Gruppenprofilmerkmale** zurückzukehren.

7. Wählen Sie die Option **Speichern** im Menü **Profil** des Fensters **Gruppenprofilmerkmale** aus, um die Änderungen am Profil zu speichern.

Befehlszeile

Um die Standardwertegruppen für ein Gruppenprofil über die Befehlszeile festzulegen, listen Sie die Attributarten in einem angegebenen Profil mit dem Befehl **wlspolm** auf. Mit dem Befehl **wgetpolm** legen Sie dann die aktuelle Standardwertegruppe für ein angegebenes Attribut fest. Anschließend können Sie mit dem Befehl **wputpolm** die Standardwertegruppe für das Attribut ändern.

Im folgenden Beispiel werden die Attribute für ein Gruppenprofil aufgelistet:

```
wlspolm @GroupProfile:developers
```

Dabei gilt Folgendes:

@GroupProfile:developers
Gibt das Profil an, dessen Attribute aufgelistet werden sollen.

Die folgende Liste wird zurückgegeben:

```
comment
GID
name
fixed
users
```

Im folgenden Beispiel wird die momentan definierte Standardwertegruppe für ein angegebenes Attribut des Gruppenprofils zurückgegeben:

```
wgetpolm -d @GroupProfile:developers gid
```

Im folgenden Beispiel wird die Standardwertegruppe für ein Gruppenprofil gesetzt:

```
wputpolm -d -c 10 @GroupProfile:developers gid
```

Dabei gilt Folgendes:

-d Setzt die Standardwertegruppe.

-c 10 Gibt 10 als den konstanten Wert für die neue Standardwertgruppe an.

@GroupProfile:developers
Gibt den Namen des Profils an, für das eine Richtlinie gesetzt werden soll.

gid Gibt das Attribut an, für das eine Richtlinie gesetzt wird.

Informationen zum Editieren von Standardwertegruppen von Gruppen über die Befehlszeile finden Sie in der Beschreibung der Befehle **wgetpolm**, **wputpolm** und **wlspolm** im Handbuch *Tivoli Framework Reference Guide*.

Richtlinie für Gültigkeitsprüfung definieren

Bei der Einrichtung von Gruppenprofilen können Sie für jedes Profil Richtlinien für Gültigkeitsprüfung definieren.

Sie können für jedes Attribut von Gruppendatensätzen auch festlegen, ob Profilsubskribenten die Richtlinie für Gültigkeitsprüfung in ihren lokalen Kopien der verteilten Profile ändern können.

Anmerkung: Im folgenden Abschnitt wird lediglich das Einrichten der Richtlinien für Gültigkeitsprüfung beschrieben. Die Überprüfung der Datensätze anhand der Profilrichtlinie wird nicht erläutert. Informationen zur Überprüfung von Datensätzen anhand der Profilrichtlinien finden Sie im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

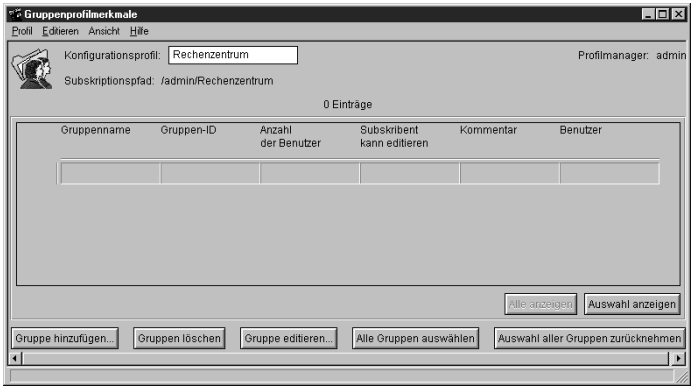
Aktivität	Umgebung	Berechtigungsklasse
Richtlinien für Gültigkeitsprüfung von Gruppenprofilen editieren	Gruppenprofil	**senior**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Richtlinien für Gültigkeitsprüfung von Gruppenprofilen zu editieren:

1. Klicken Sie in einem Profilmanager doppelt auf das Symbol eines Gruppenprofils, um das Fenster **Gruppenprofilmerkmale** anzuzeigen.



2. Wählen Sie **Richtlinien für Gültigkeitsprüfung** im Menü **Editieren** aus, um den Dialog **Richtlinien für Gültigkeitsprüfung editieren** anzuzeigen.

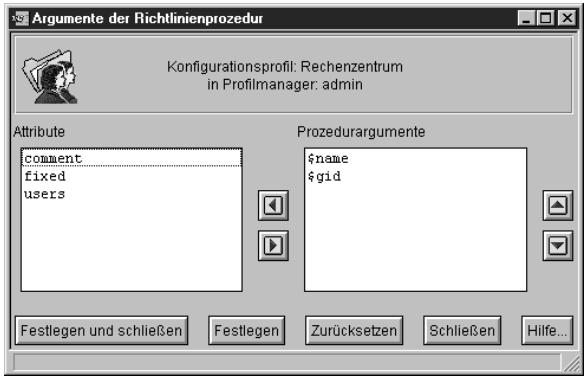
3. Wählen Sie ein Attribut in der Liste **Attribute** aus.
4. Klicken Sie auf das Optionsfeld **Ja** im Feld **Subskribenten können Richtlinie editieren**, damit Subskribenten Änderungen durchführen können. Klicken Sie andernfalls auf das Optionsfeld **Nein**.

5. Wählen Sie eine Gültigkeitsart in der Dropdown-Liste **Standardart** aus. Die verfügbaren Optionen lauten: **Keine**, **Konstante** oder **Skript** (früher: Prozedur).

   Wenn Sie die Option **Konstante** auswählen, geben Sie einen konstanten Wert in das Feld **Wert** ein.

   Führen Sie folgende Schritte aus, wenn Sie die Option **Skript** ausgewählt haben:

   a. Klicken Sie auf **Skriptargumente editieren...** (früher: Prozedurargumente editieren...), um den Dialog **Argumente des Richtlinienskripts** (früher: Argumente der Richtlinienprozedur) anzuzeigen. Bestimmen Sie mit diesem Dialog die Reihenfolge der Skriptargumente.

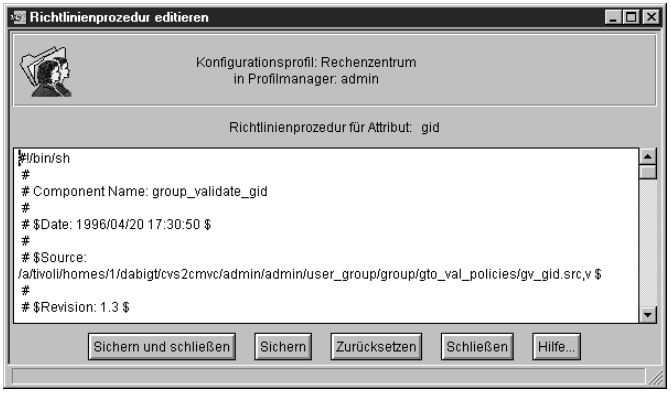


   b. Wählen Sie die Datensatzattribute, die die Skriptargumente für das Richtlinienskript des aktuellen Attributs werden sollen, in der Liste **Attribute** aus. Klicken Sie auf den Rechtspfeil, um die Attribute in die Liste **Skriptargumente** (früher: Prozedurargumente) zu verschieben.

      Sie können die Reihenfolge ändern, in der ein Argument aufgerufen wird, indem Sie das Argument auswählen und auf den Aufwärtspfeil bzw. den Abwärtspfeil klicken, um das Argument an die gewünschte Position zu verschieben.

   c. Klicken Sie auf **Festlegen und schließen**, um die neuen Argumente hinzuzufügen und zum Dialog **Richtlinien für Gültigkeitsprüfung editieren** zurückzukehren.

d. Klicken Sie im Dialog **Richtlinien für Gültigkeitsprüfung editieren** auf **Skripthauptteil editieren** (früher: Prozedurhauptteil editieren), um den Dialog **Richtlinienskript editieren** (früher: Richtlinienprozedur editieren) anzuzeigen.



e. Geben Sie den Hauptteil des Skripts ein.

f. Klicken Sie auf **Speichern und schließen** (früher: Sichern und schließen), um das Skript in der Datenbank zu speichern und zum Dialog **Richtlinien für Gültigkeitsprüfung editieren** zurückzukehren.

Wiederholen Sie den vorherigen Vorgang für jedes Attribut des Datensatzes.

6. Klicken Sie auf **Festlegen und schließen**, um die Änderungen anzuwenden und zum Fenster **Gruppenprofilmerkmale** zurückzukehren.

7. Wählen Sie die Option **Speichern** im Menü **Profil** des Fensters **Gruppenprofilmerkmale** aus, um die Änderungen am Profil zu speichern.

Befehlszeile

Um die Richtlinien für Gültigkeitsprüfung für ein Gruppenprofil über die Befehlszeile festzulegen, listen Sie die Attributarten in einem angegebenen Profil mit dem Befehl **wlspolm** auf. Mit dem Befehl **wgetpolm** legen Sie dann die aktuelle Richtlinie für ein angegebenes

Attribut fest. Anschließend können Sie mit dem Befehl **wputpolm** die Richtlinie für das Attribut ändern.

Im folgenden Beispiel werden die Attribute für ein Gruppenprofil aufgelistet:

```
wlspolm @GroupProfile:testers
```

Dabei gilt Folgendes:

@GroupProfile:testers
Gibt den Namen des Profils an, dessen Attribute aufgelistet werden sollen.

Die folgende Liste wird zurückgegeben:

```
comment
GID
name
fixed
users
```

Im folgenden Beispiel wird die momentan definierte Richtlinie für Gültigkeitsprüfung für ein angegebenes Attribut des Gruppenprofils zurückgegeben:

```
wgetpolm -v @GroupProfile:testers gid
```

Im folgenden Beispiel wird die Gültigkeitsprüfung für ein Gruppenprofil inaktiviert. Das Attribut kann also einen beliebigen Wert annehmen:

```
wputpolm -v -n @GroupProfile:testers gid
```

Dabei gilt Folgendes:

-v Setzt die Richtlinie für Gültigkeitsprüfung fest.

-n Inaktiviert die Gültigkeitsprüfung für das angegebene Attribut.

@GroupProfile:testers
Gibt den Namen des Profils an, für das eine Richtlinie gesetzt werden soll.

gid Gibt das Attribut an, für das eine Richtlinie gesetzt wird.

Informationen zum Editieren der Richtlinie für Gültigkeitsprüfung von Gruppen über die Befehlszeile finden Sie in der Beschreibung der Befehle **wgetpolm**, **wputpolm** und **wlspolm** im Handbuch *Tivoli Framework Reference Guide*.

Gruppenprofile verwalten

Nachdem Sie Gruppenprofile erstellt und eingerichtet haben, müssen Sie vorhandene Gruppen möglicherweise an das Profil weitergeben. Außerdem können Sie die Gruppendatensätze neu sortieren, um die vorhandenen Gruppeninformationen zu überprüfen, und Sie können die Standardwerte steuern, die ein Profil verwendet, wenn Tivoli SecureWay User Administration das Profil verteilt.

Daten an Gruppenprofile weitergeben

Bei der Weitergabe von Daten an ein Gruppenprofil (d. h. beim Füllen der Gruppenprofile mit Daten) werden Benutzerinformationen zu Gruppen vom angegebenen System in die Tivoli-Gruppendatensätze des aktuellen Profils importiert.

Anmerkung: Bei der Datenweitergabe aus einer UNIX-TMR werden Kennwörter zur Verfügung gestellt, die anders als die Kennwörter anderer Plattformen verarbeitet werden. Weitere Informationen zur Verarbeitung der Kennwörter während des Weitergabevorgangs finden Sie unter „Kennwortsteuerung” auf Seite 28.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

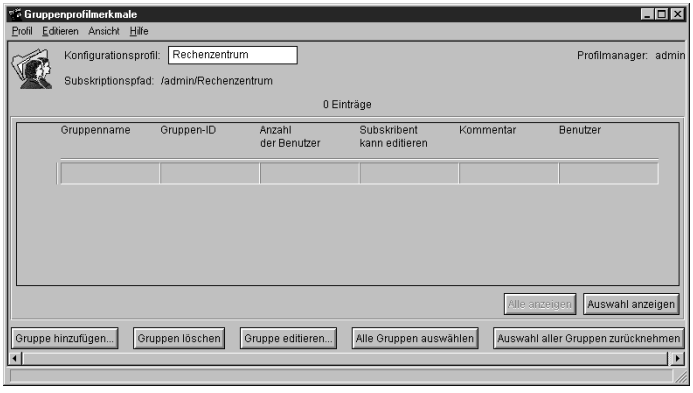
Aktivität	Umgebung	Berechtigungsklasse
Daten an Gruppenprofil weitergeben	Profilmanager	**admin**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Daten an ein Gruppenprofil weiterzugeben:

1. Klicken Sie in einem Profilmanager doppelt auf das Symbol eines Gruppenprofils, um das Fenster **Gruppenprofilmerkmale** anzuzeigen.



2. Wählen Sie **Ausfüllen** aus dem Menü **Profil** aus, um den Dialog **Profil ausfüllen** aufzurufen.

3. Wählen Sie in der Liste **Keine Datensätze von diesen verwalteten Knoten und NIS-Domänen abrufen** die Tivoli-Ressourcen aus, aus denen Daten an das Profil weitergegeben werden sollen. Wenn Sie Ressourcen unterschiedlicher Art auswählen, fügt Tivoli die verschiedenen Standardsystemkonten im Profil zusammen.

4. Klicken Sie auf den Linkspfeil, um die ausgewählten Ressourcen in die Liste **Datensätze von diesen verwalteten Knoten und NIS-Domänen abrufen** zu verschieben.
5. Klicken Sie auf eines der folgenden Optionsfelder:
   - **An vorhandene Datensatzliste anhängen** Fügt die neuen Datensätze den vorhandenen Datensätzen im Profil hinzu. Verwenden Sie diese Option, wenn Sie Daten an ein Profil weitergeben, welches Datensätze enthält, die Sie beibehalten möchten.
   - **Vorhandene Datensatzliste überschreiben** Ersetzt den Inhalt des Gruppenprofils durch die neuen Datensätze.

     Anmerkung: Verwenden Sie diese Option mit Bedacht, da alle vorhandenen Datensätze im Profil verloren gehen.
6. Klicken Sie auf **Ausfüllen und schließen**, um die Datensätze hinzuzufügen und den Dialog zu schließen.

   Tivoli SecureWay User Administration fügt dem Profil die Konten aus den angegebenen Systemen hinzu.
7. Wählen Sie die Option **Speichern** im Menü **Profil** des Fensters **Gruppenprofilmerkmale** aus, um die Änderungen am Profil zu speichern.

Befehlszeile

Im folgenden Beispiel werden Daten an ein Gruppenprofil weitergegeben:

```
wpopgrps -o @ManagedNode:kenya @GroupProfile:developers
```

Dabei gilt Folgendes:

-o Überschreibt den aktuellen Inhalt des Gruppenprofils.

@ManagedNode:kenya
Gibt den Namen des Systems an, von dem Daten weitergegeben werden sollen.

@GroupProfile:developers
Gibt den Namen des Profils an, an das Daten weitergegeben werden sollen.

Weitere Informationen hierzu finden Sie in der Beschreibung des Befehls **wpopgrps** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Anmerkung: Für die Datenweitergabe an Gruppendateien steht die Option zum Zusammenfügen derzeit noch nicht zur Verfügung. Werden beispielsweise an ein Gruppenprofil Daten aus dem verwalteten Knoten **cougar** weitergegeben und anschließend aus dem verwalteten Knoten **puma** weitergegeben bzw. angehängt, so werden die zusätzlichen Benutzer vorhandener Gruppen *nicht* an die Liste mit den Gruppenteilnehmern aus **cougar** angehängt.

Standardwerte für Verteilung festlegen

Sie können die Standardwerte steuern, die von einem Profil bei seiner Verteilung durch Tivoli SecureWay User Administration verwendet werden. Wenn Sie ein Profil von einem Profilmanager verteilen, werden Ihnen keine Optionen dafür angeboten, wie die Verteilung ausgeführt werden soll. Stattdessen verwendet Tivoli SecureWay User Administration die Standardoptionen, die Sie mit dem Dialog **Standardwerte verteilen** definieren. Die Standardwerte bestimmen auch, welche Optionsfelder standardmäßig ausgewählt sind, wenn Sie den Dialog **Profil verteilen** entweder über das Kontextmenü des Benutzerprofils oder über die Option **Verteilen** im Fenster **Gruppenprofilmerkmale** aufrufen. Die Standardwerte werden für jedes Profil gesondert festgelegt. Die Standardoptionen jedes Profils können sich von denen anderer Profile unterscheiden.

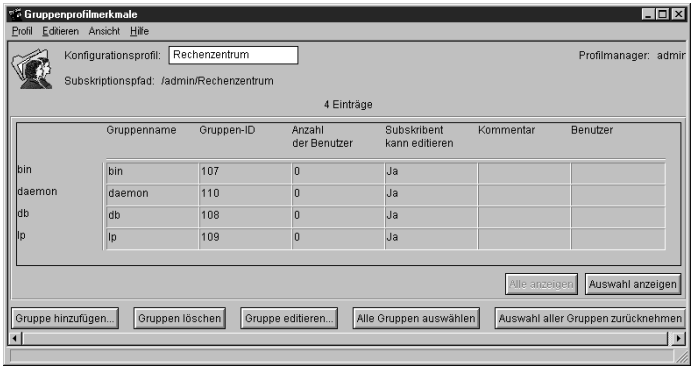
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Standardwerte für Verteilung festlegen	Profilmanager	**admin**

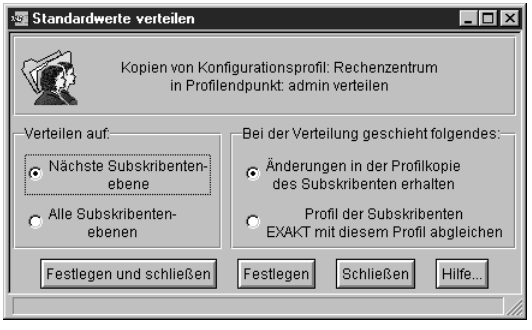
Sie können diese Task nur über die Tivoli-Arbeitsoberfläche ausführen.

Führen Sie folgende Schritte aus, um die Standardwerte eines Profils festzulegen:

1. Klicken Sie in einem Profilmanager doppelt auf das Symbol eines Gruppenprofils, um das Fenster **Gruppenprofilmerkmale** anzuzeigen.



2. Wählen Sie **Standardwerte verteilen** im Menü **Profil** aus, um den Dialog **Standardwerte verteilen** anzuzeigen.



3. Klicken Sie auf **Nächste Subskribentenebene** im Feld **Verteilen auf**, um eine Kopie des Profils nur auf die nächste Subskribentenebene zu senden. Verwenden Sie diese Option, wenn Sie die Kopien der Subskribenten nicht auf allen unteren Ebenen in der Subskriptionshierarchie ändern möchten.

   Anmerkung: Wenn die nächste Ebene der Subskribenten die Ebene des verwalteten Knotens ist, wird das Profil nur an den Tivoli-verwalteten Knoten verteilt und nicht an die eigentlichen Systemdateien. Wenn Sie die Systemdateien mit Hilfe dieser Option ändern möchten, müssen Sie das Profil von der Ebene des verwalteten Knotens verteilen.

   — ODER —

   Klicken Sie auf **Alle Subskribentenebenen**, um eine Kopie des Profils an die nächste Ebene der Subskribenten und deren Subskribenten zu senden. Verwenden Sie diese Option, wenn Sie alle Subskribenten auf der unteren Ebene in der Subskriptionshierarchie einschließlich der Systemdateien der Profilendpunkte ändern möchten.

4. Klicken Sie auf **Änderungen in der Profilkopie des Subskribenten erhalten** im Feld **Bei der Verteilung geschieht folgendes:**, um Änderungen beizubehalten, die Administratoren an den Profilen vorgenommen haben, deren Profilmanager dem aktuellen Profil zugeordnet sind. Verwenden Sie diese Option, wenn Profile in Subskribenten definiert wurden, deren Unterschiede Sie beibehalten möchten.

   — ODER —

   Klicken Sie auf das Optionsfeld **Profil des Subskribenten EXAKT mit diesem Profil abgleichen**, um die Änderungen, die Administratoren an ihren Profilen vorgenommen haben, mit den in diesem Profil definierten Werten zu überschreiben. Verwenden Sie diese Option, wenn Sie die Unterschiede zwischen den Profilen der Subskribenten nicht beibehalten möchten.

Anmerkung: Wenn Sie dieses Optionsfeld verwenden, wird der gesamte Profilinhalt auf den Endpunkt geschrieben. Alle vorgenommenen Änderungen werden überschrieben.

5. Klicken Sie auf **Festlegen und schließen**, um die Standardoptionen festzulegen und zum Dialog **Gruppenprofilmerkmale** zurückzukehren.

9

Gruppendatensätze verwalten

Die Informationen der Gruppendatensätze sind in einer Gruppenprofildatenbank gespeichert. Die neuen Gruppenkontoinformationen werden Systemdateien erst dann hinzugefügt, wenn Sie das Profil an das endgültige Ziel verteilen. Sie können die Datensätze nacheinander mit dem Dialog **Datensatz zu Profil hinzufügen** erstellen.

In diesem Abschnitt erfahren Sie, wie die Gruppenkontodatensätze verwaltet werden. Folgende Themen werden beschrieben:

- Einen Gruppendatensatz erstellen
- Gruppendatensatz editieren
- Gruppendatensätze anhand der Richtlinien überprüfen
- Gruppendatensatz löschen
- Gruppenprofile an Subskribenten verteilen
- Kopien von Gruppendatensätzen mit der Tivoli-Datenbank abrufen
- Gruppendatensätze mit der Tivoli-Datenbank synchronisieren

Neue Datensätze für Gruppenkonten erstellen

Datensätze für Gruppenkontos enthalten alle Informationen, die für das Verwalten eines Gruppenkonten benötigt werden. Wenn Sie einen neuen Datensatz für ein Gruppenkonto erstellen, speichert Tivoli SecureWay User Administration die Kontoinformationen in einer Gruppenprofildatenbank. Die neuen Gruppenkontoinformationen werden Systemdateien erst dann hinzugefügt, wenn Sie das Profil an das endgültige Ziel verteilen. Sie können die Datensätze mit dem Dialog **Datensatz dem Profil hinzufügen** nacheinander erstellen.

Sie können den Feldern jedes Gruppendatensatzes die folgenden Informationsarten hinzufügen:

- Gruppenname
- Gruppen-ID (GID)
- Kommentare zur Gruppe
- Gruppenmitglieder
- Ob die Subskribenten den Datensatz ändern können

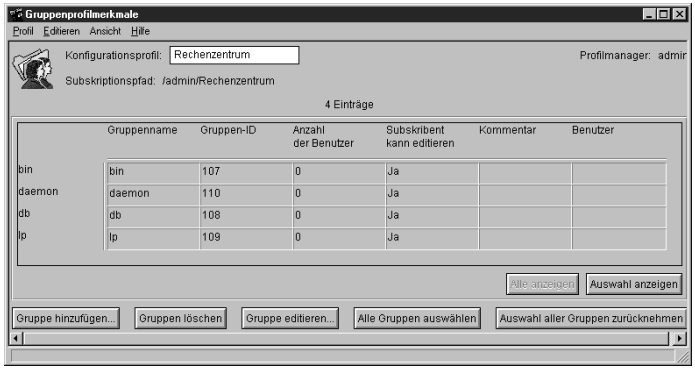
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Datensatz eines Gruppenkontos erstellen	Gruppenprofil	**admin**

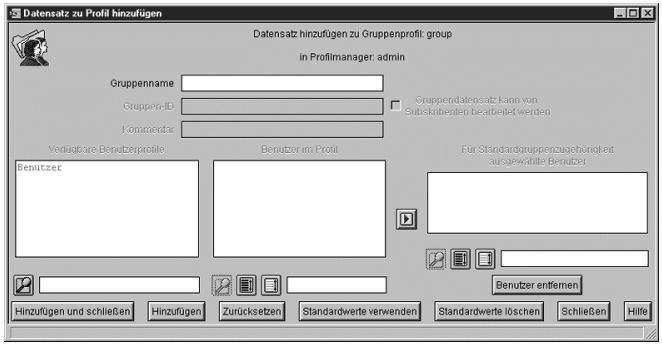
Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

1. Klicken Sie in einem Profilmanager doppelt auf das Gruppenprofil, dem Sie die neue Gruppe hinzufügen möchten. Das Fenster **Gruppenprofilmerkmale** wird angezeigt.



2. Klicken Sie auf **Gruppe hinzufügen**, um den Dialog **Datensatz zu Profil hinzufügen** anzuzeigen.



3. Geben Sie den Gruppennamen in das Feld **Gruppenname** ein. Namen dürfen nur alphanumerische Zeichen, Punkte (.), Unterstreichungszeichen (_), Bindestriche (–) und Leerzeichen ( ) enthalten. Andere Zeichen sind nicht zulässig.

   Anmerkung: Wenn Sie die von Tivoli bereitgestellten Standardwertegruppen verwenden, können Sie auf **Standardwerte verwenden** klicken, um den Rest der Dialogfelder mit den Standardwerten zu füllen. Wenn Sie auf **Standardwerte verwenden** klicken, nachdem Sie Informationen in ein Feld eingegeben haben, für das eine Standardwertegruppe definiert ist, ersetzt Tivoli SecureWay

User Administration Ihre Informationen durch die Informationen aus der Standardwertegruppe. Ändern Sie anschließend nach Bedarf die Werte in den Feldern. Wenn Richtlinien für Gültigkeitsprüfung verwendet werden, müssen die von Ihnen gewählten Werte die Gültigkeitsprüfung für die Felder durchlaufen, deren Richtlinien auf Gültigkeit geprüft werden. Wenn die Werte nicht gültig sind, wird der Datensatz dem Profil nicht hinzugefügt.

4. Klicken Sie auf **Standardwerte verwenden**.
5. Geben Sie die Identifikationsnummer der Gruppe (GID) in das Feld **Gruppen-ID** ein.
6. Geben Sie die Kommentare zur Gruppe in das Feld **Kommentar** ein.
7. Wenn Sie möchten, dass die Subskribenten diesen Datensatz editieren können, aktivieren Sie das Kontrollkästchen **Gruppendatensatz kann von Subskribenten bearbeitet werden**.
8. Wählen Sie ein Benutzerprofil, aus dem Benutzerkontoinformationen für die Gruppe abgerufen werden sollen, in der Liste **Verfügbare Benutzerprofile** aus.
9. Wählen Sie die Benutzerdatensätze, deren Namen Sie dem Gruppendatensatz hinzufügen möchten, in der Liste **Benutzer im Profil** aus.
10. Klicken Sie auf den Rechtspfeil, um die Benutzerdatensätze dem Gruppendatensatz hinzuzufügen.
11. Wiederholen Sie die Schritte 8, 9 und 10, um Mitglieder aus anderen Profilen im aktuellen Profilmanager hinzuzufügen.
12. Nehmen Sie erforderliche Änderungen am Datensatz vor.
13. Klicken Sie auf **Hinzufügen und schließen**, um den Datensatz hinzuzufügen und zum Gruppenprofil zurückzukehren.
14. Wählen Sie die Option **Speichern** im Menü **Profil** des Fensters **Gruppenprofilmerkmale** aus, um die Änderungen an der Profildatenbank zu speichern.

Befehlszeile

Im folgenden Beispiel wird ein Gruppendatensatz erstellt:

```
wcrtgrp -u dgates, jgriffin, rroyer \
@GroupProfile:developers
```

Dabei gilt Folgendes:

-u dgates, ...
Gibt die Anmeldenamen der Benutzer an, die der Gruppe hinzugefügt werden sollen.

@GroupProfile:developers
Gibt den Namen des Profils an, dem der Gruppendatensatz hinzugefügt wird.

Weitere Informationen hierzu finden Sie in der Beschreibung des Befehls **wcrtgrp** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Gruppenkontodatensätze editieren

Wenn Sie den Datensatz eines vorhandenen Gruppenkontos ändern, speichert Tivoli SecureWay User Administration die Kontoinformationen in einer Gruppenprofildatenbank. Die Gruppenkontoinformationen werden Systemdateien erst dann hinzugefügt, wenn Sie das Profil an das endgültige Ziel verteilen.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

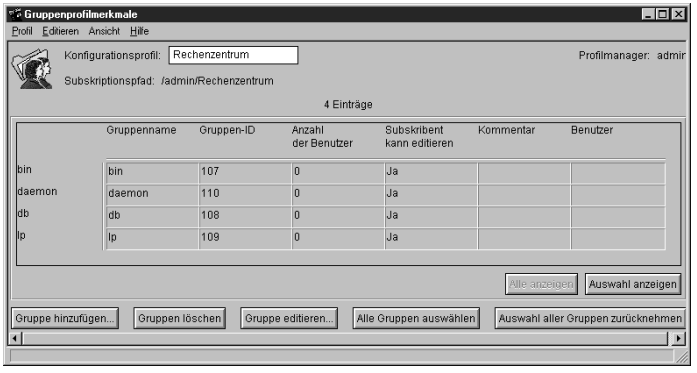
Aktivität	Umgebung	Berechtigungsklasse
Gruppenkontodatensatz editieren	Gruppenprofil	**admin**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

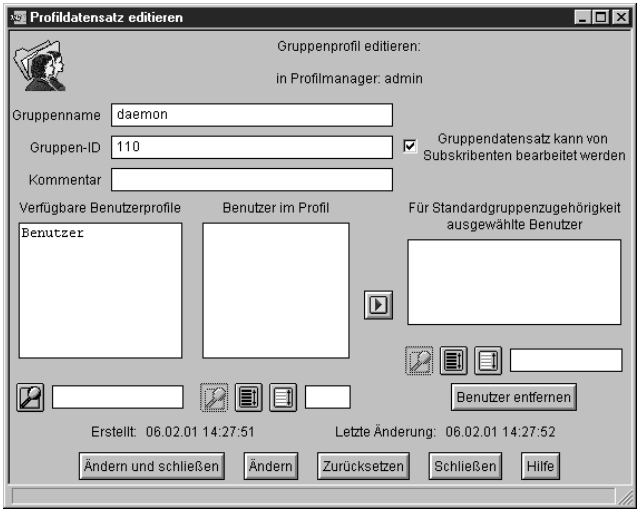
Arbeitsoberfläche

Führen Sie folgende Schritte aus, um den Datensatz eines Gruppenkontos zu editieren:

1. Klicken Sie in einem Profilmanager doppelt auf das Symbol eines Gruppenprofils, um das Fenster **Gruppenprofilmerkmale** anzuzeigen.



2. Klicken Sie doppelt auf einen Gruppendatensatz, um den Dialog **Profildatensatz editieren** anzuzeigen.



3. Ändern Sie beliebig die folgenden Gruppenkontoinformationen:
   - Den Gruppennamen im Feld **Gruppenname**
   - Die Identifikationsnummer der Gruppe (GID) im Feld **Gruppen-ID**
   - Ob Subskribenten diesen Datensatz editieren können; aktivieren Sie dazu das Kontrollkästchen **Gruppendatensatz kann von Subskribenten bearbeitet werden** aus
   - Die Anzahl der Benutzerdatensätze im Gruppendatensatz
4. Klicken Sie auf **Ändern und schließen**, um den Datensatz zu ändern und zum Gruppenprofil zurückzukehren.
5. Wählen Sie die Option **Speichern** im Menü **Profil** des Fensters **Gruppenprofilmerkmale** aus, um die Änderungen an der Profildatenbank zu speichern.

Befehlszeile

Zum Ändern der Attribute eines Gruppendatensatzes können Sie zunächst die aktuellen Werte der Datensatzattribute mit dem Befehl **wgetgrp** auflisten. Anschließend können Sie diese mit dem Befehl **wsetgrp** ändern. Sie können auch den Befehl **wrmusrg** verwenden, um Benutzer aus dem Gruppendatensatz zu entfernen.

Im folgenden Beispiel werden alle Attribute eines Gruppendatensatzes aufgelistet:

```
wgetgrp @GroupProfile:developers "Who"
```

Dabei gilt Folgendes:

GroupProfile:developers
: Gibt den Namen des Profils an, dessen Datensatzattribute aufgelistet werden.

“Who”
: Gibt den Namen des Gruppendatensatzes an, dessen Attribute aufgelistet werden.

Befehlsausgabe:

```
Name: Who
GID: 105
Kommentar: British
Benutzer: 4
Gruppendatensatz ist fixiert: FALSE
```

Im folgenden Beispiel werden alle Attribute eines Gruppendatensatzes festgelegt:

```
wsetgrp -C "UNIX developers" -F @GroupProfile:developers \ "Who"
```

Dabei gilt Folgendes:

-C “UNIX developers”
Gibt einen Kommentar zum Gruppendatensatz an.

-F Verhindert, dass Subskribenten den Datensatz ändern.

@GroupProfile:developers
Gibt den Namen des Profils an, dessen Datensatz geändert wird.

“Who”
Gibt den Namen des zu ändernden Datensatzes an.

Im folgenden Beispiel wird ein Mitglied aus einem Gruppendatensatz gelöscht:

```
wrmusrg @GroupProfile:developers "Who" kmoon
```

Dabei gilt Folgendes:

@GroupProfile:developers
Gibt den Namen des Gruppenprofils an, das den Gruppendatensatz enthält, dessen Mitglied gelöscht werden soll.

“Who”
Gibt den Namen des Gruppendatensatzes an, dessen Mitglied gelöscht werden soll.

kmoon
Gibt den Namen des zu löschenden Gruppenmitglieds an.

Weitere Informationen zum Editieren der Attribute eines Gruppenkontodatensatzes über die Befehlszeile finden Sie in der Beschreibung der Befehle **wsetgrp** und **wrmusrg** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Gruppenkontodatensatz löschen

Wenn Sie ein Gruppenkonto nicht mehr benötigen, können Sie es aus dem Profil löschen. Wenn Sie das Profil dann erneut verteilen, wird der Datensatz bei allen Subskribenten gelöscht, die die neue Profilkopie erhalten.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

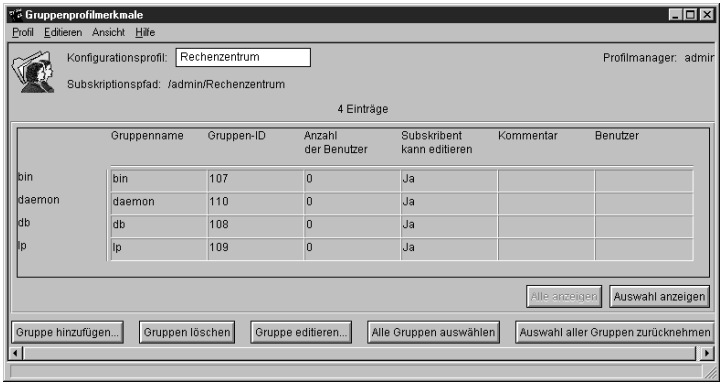
Aktivität	Umgebung	Berechtigungsklasse
Gruppenkontodatensatz löschen	Gruppenprofil	**admin**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um einen Gruppendatensatz zu löschen:

1. Klicken Sie in einem Profilmanager doppelt auf das Symbol eines Gruppenprofils, um das Fenster **Gruppenprofilmerkmale** anzuzeigen.



2. Wählen Sie die zu löschenden Gruppenkonten aus.

   Anmerkung: Sie können einen Datensatz auswählen, indem Sie mit der rechten Maustaste darauf klicken. Sie können mehrere Datensätze auswählen, indem Sie einen Datensatz auswählen und den Mauszeiger nach oben oder nach unten über die Profileinträge ziehen, indem Sie die Taste **Strg** drücken und mehrere Datensätze auswählen oder indem Sie den Dialog **Datensätze suchen** verwenden.

3. Klicken Sie auf **Gruppen löschen**, um die ausgewählten Datensätze aus dem Profil zu löschen.

4. Wählen Sie die Option **Speichern** im Menü **Profil** des Fensters **Gruppenprofilmerkmale** aus, um die Änderungen an der Profildatenbank zu speichern.

Befehlszeile

Im folgenden Beispiel wird ein Datensatz aus einem Gruppenprofil gelöscht:

```
wdelgrp @GroupProfile:developers dgates
```

Dabei gilt Folgendes:

GroupProfile:developers
: Gibt den Namen des Profils an, das den zu löschenden Gruppendatensatz enthält.

dgates
: Gibt den Namen der zu löschenden Gruppe an.

Weitere Informationen hierzu finden Sie in der Beschreibung des Befehls **wdelgrp** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Gruppenprofile an Subskribenten verteilen

Nachdem Sie ein Gruppenprofil erstellt und ihm Datensätze hinzugefügt haben, können Sie Kopien des Profils an die Subskribenten seines Profilmanagers verteilen. Die Subskribenten können UNIX-verwaltete Knoten, UNIX-Endpunkte, NIS-Domänen und andere Profilmanager sein. Wenn Sie die Kopie eines Profils an einen anderen Profilmanager verteilen und die Datensätze im Originalprofil nicht gesperrt sind, kann der Administrator des zweiten Profilmanagers lokale Änderungen an der Subskribentenkopie des Profils vornehmen. Anschließend kann der Administrator das geänderte Profil an Subskribentensysteme und NIS-Domänen verteilen. Erst wenn Profilinformationen an Subskribentensysteme und NIS-Domänen verteilt werden, werden die Systemdateien und NIS-Listen geändert. Bis dahin werden keine Gruppenkonten auf Systemebene hinzugefügt oder geändert.

Weitere Informationen zum Subskribieren von Tivoli-Ressourcen für Profilmanager finden Sie im *Tivoli Management Framework Benutzerhandbuch*.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

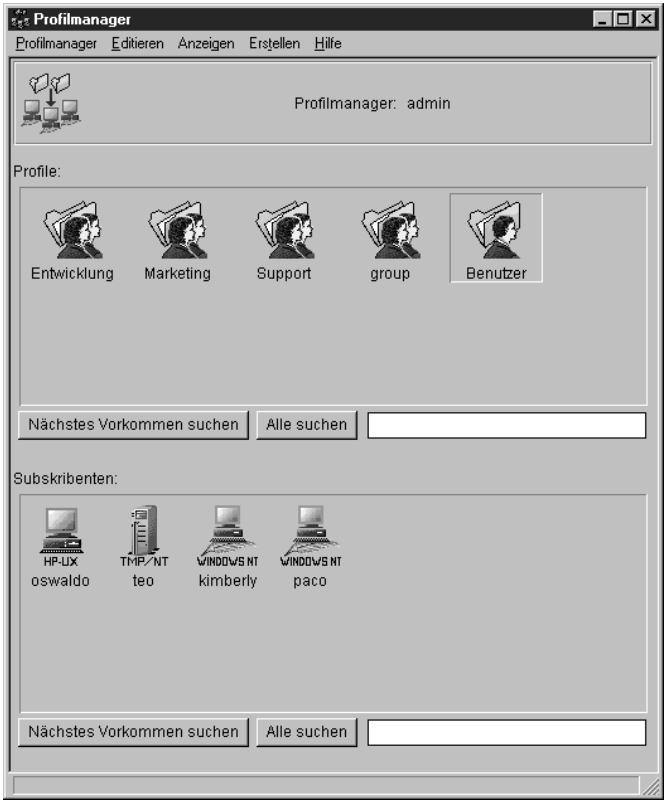
Aktivität	Umgebung	Berechtigungsklasse
Gruppenprofile an Subskribenten verteilen	Subskribenten-Richtlinienbereich	**admin**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Gruppenprofile an Subskribenten von einem Profil aus zu verteilen:

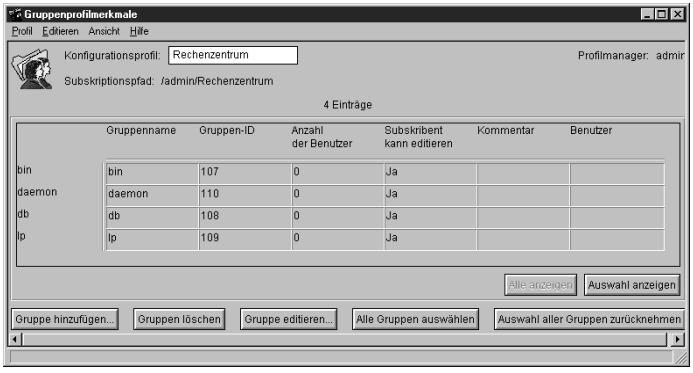
1. Klicken Sie in einem Richtlinienbereich doppelt auf das Symbol eines Profilmanagers, um das Fenster **Profilmanager** anzuzeigen.



2. Fügen Sie die erforderlichen Subskribenten dem Profilmanager hinzu.

   Informationen zum Subskribieren von Ressourcen für Profilmanager finden Sie im *Tivoli Management Framework Benutzerhandbuch*.

3. Klicken Sie doppelt auf das Symbol eines Gruppenprofils, um das Fenster **Gruppenprofilmerkmale** anzuzeigen.



4. Wählen Sie im Menü **Profil** die Option **Verteilen** aus (wenn die Option **Verteilen** inaktiv ist, speichern Sie das Profil, und versuchen Sie es erneut), um den Dialog **Profil verteilen** anzuzeigen.

5. Klicken Sie auf **Nächste Subskribentenebene** im Feld **Verteilen an** (früher: Verteilen auf), um eine Kopie des Profils nur auf die nächste Subskribentenebene zu senden. Verwenden Sie diese Option, wenn Sie die Kopien der Subskribenten nicht auf allen unteren Ebenen in der Subskriptionshierarchie ändern möchten.

Anmerkung: Wenn die nächste Ebene der Subskribenten die Ebene des verwalteten Knotens ist, wird das Profil nur an den Tivoli-verwalteten Knoten verteilt und nicht an die Systemdateien. Zum Ändern der Systemdateien mit dieser Option müssen Sie das Profil von der Ebene des verwalteten Knotens verteilen.

— ODER —

Klicken Sie auf **Alle Subskribentenebenen**, um eine Kopie des Profils an die nächste Ebene der Subskribenten seines Profilmanagers und deren Subskribenten zu senden. Verwenden Sie diese Option, wenn Sie alle Subskribenten auf der unteren Ebene in der Subskriptionshierarchie einschließlich der Systemdateien der Profilendpunkte ändern möchten.

6. Klicken Sie auf **Änderungen in der Profilkopie des Subskribenten erhalten**, um Änderungen beizubehalten, die Administratoren an den Profilen vorgenommen haben, deren Profilmanager diesem Profil zugeordnet sind. Verwenden Sie diese Option, wenn Sie Profile in Subskribenten besitzen möchten, deren Unterschiede Sie beibehalten möchten.

   — ODER —

   Klicken Sie auf das Optionsfeld **Profil des Subskribenten EXAKT mit diesem Profil abgleichen**, um die Änderungen, die Administratoren an ihren Profilen vorgenommen haben, mit den in diesem Profil definierten Werten zu überschreiben. Verwenden Sie diese Option, wenn Sie die Unterschiede zwischen den Profilen der Subskribenten nicht beibehalten möchten.

   Anmerkung: Die Option **Profil des Subskribenten EXAKT mit diesem Profil abgleichen** überschreibt jede Änderung und ersetzt alles in den Systemdateien und NIS-Listen außer im **root**-Konto

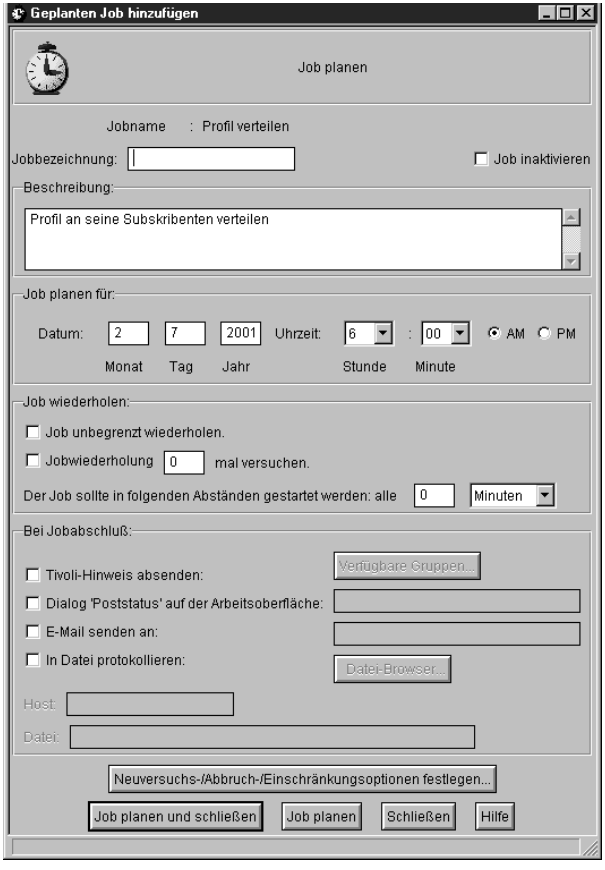
7. Wählen Sie in der Liste **Keine Verteilung an diese Subskribenten** die Subskribenten des Profilmanagers aus, an die Kopien dieses Profils verteilt werden sollen.

Klicken Sie auf den Linkspfeil, um die ausgewählten Subskribenten in die Liste **Verteilung an diese Subskribenten** zu verschieben.

8. Klicken Sie auf **Verteilen und schließen**, um das Profil sofort zu verteilen und zum Fenster **Gruppenprofilmerkmale** zurückzukehren.

   — ODER —

   Klicken Sie auf **Planen**, um den Dialog **Geplanten Job hinzufügen** anzuzeigen.



Befehlszeile

Im folgenden Beispiel wird ein Gruppenprofil an einen zugeordneten verwalteten Knoten verteilt:

```
wdistrib -l maintain @GroupProfile:developers \
@ManagedNode:kenya
```

Dabei gilt Folgendes:

-l maintain
: Behält alle lokalen Änderungen in den Subskribentenkopien des Profils bei.

-m
: Gibt eine Verteilung in mehreren Schritten an. Das Profil wird an alle Ebenen der Subskribenten verteilt, einschließlich der Systemdateien.

@UserProfile:developers
: Gibt den Namen des Profils an, das verteilt werden soll.

@ManagedNode:kenya
: Gibt den Namen des Subskribenten an, an den das Profil verteilt werden soll.

Weitere Informationen zur Verteilung von Gruppenprofilinformationen und zu deren Planung finden Sie in der Beschreibung der Befehle **wdistrib** und **wschedjob** im Handbuch *Tivoli Framework Reference Manual*.

Kopien von Gruppenprofilen aus einem anderen Profil abrufen

Sie können eine neue Kopie eines Profils aus dem Profilmanager abrufen, der sich in der Subskriptionshierarchie eine Ebene höher befindet. Dies kann hilfreich sein, wenn Sie auf einer unteren Ebene arbeiten und auf Ihrer aktuellen Ebene die Kopie eines Profils von einer höheren Ebene anfordern möchten. Dieser Vorgang ist im Kern eine Anfrage an den zugeordneten Profilmanager auf Verteilung an einen einzelnen Subskribenten.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

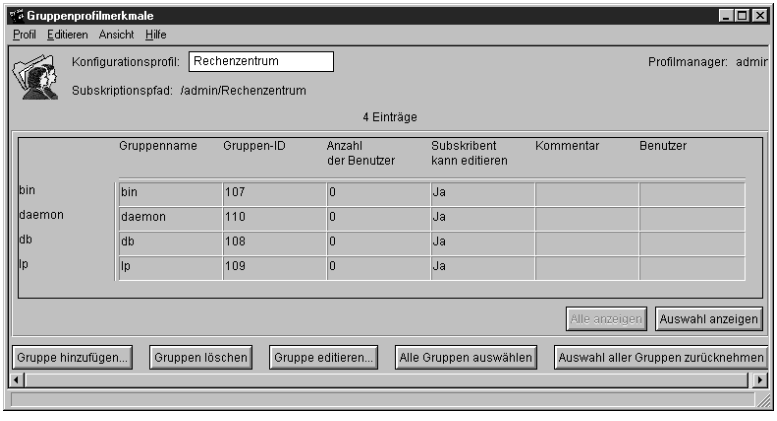
Aktivität	Umgebung	Berechtigungsklasse
Gruppenprofilkopien aus einem anderen Profil abrufen	Gruppenprofil	**admin**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

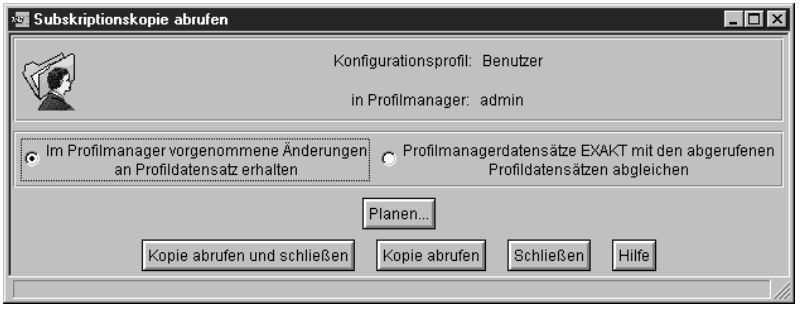
Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Gruppenprofilkopien aus einem anderen Profil abzurufen:

1. Klicken Sie in einem Profilmanager doppelt auf das Symbol eines Gruppenprofils, um das Fenster **Gruppenprofilmerkmale** anzuzeigen.



2. Wählen Sie **Neue Kopie abrufen** im Menü **Profil** aus, um den Dialog **Subskriptionskopie abrufen** anzuzeigen.



Anmerkung: Die Option **Neue Kopie abrufen** steht nur zur Auswahl, wenn die Kopie eines verteilten Gruppenprofils geöffnet ist.

3. Klicken Sie auf **Im Profilmanager vorgenommene Änderungen an Profildatensatz erhalten**, um das Profil abzurufen und die Werte im aktuellen Profil beizubehalten. Verwenden Sie diese Option, wenn Sie die Einstellungen in Ihrem Profil nach dem Abrufen des neuen Profils beibehalten möchten.

   — ODER —

   Klicken Sie auf **Profilmanagerdatensätze EXAKT mit den abgerufenen Profildatensätzen abgleichen**, um das Profil abzurufen und die Werte im aktuellen Profil zu überschreiben. Verwenden Sie diese Option, wenn Sie die lokalen Änderungen an dem aktuellen Profil nicht beibehalten möchten.

4. Damit Sie das Profil zu einem späteren Zeitpunkt abrufen können, klicken Sie auf **Planen**, um den Dialog **Geplanten Job hinzufügen** anzuzeigen.

   Weitere Informationen zur Tivoli-Planungsfunktion finden Sie im *Tivoli Management Framework Benutzerhandbuch*.

5. Klicken Sie auf **Kopie abrufen und schließen**, um sofort Kopien der Profildatensätze in das aktuelle Profil zu holen und den Dialog zu schließen.

Befehlszeile

Im folgenden Beispiel wird die Kopie eines Profils aus einem anderen Profilmanager abgerufen:

```
wgetprf -l maintain @ProfileManager:testers
```

Dabei gilt Folgendes:

- l maintain
: Behält die lokalen Änderungen in den Profilkopien der Subskribenten bei.

@ProfileManager:testers
: Gibt den Namen des Subskribenten an, für den die neue Profilkopie abgerufen wird.

Informationen zum Abrufen der Gruppenprofilinformationen aus einem anderen Profil mit Hilfe der Befehlszeile finden Sie in der Beschreibung des Befehls **wgetprf** im Handbuch *Tivoli Framework Reference Manual*.

Profildatenbank mit Systemdateien synchronisieren

Wenn die Systemkonfigurationsdateien direkt editiert werden, stimmt das Profil nicht mehr mit den Systemdateien überein, für die es die Informationen bereitstellt. Das Synchronisieren des Profils und seiner zugehörigen Datenbank mit Systemdateien zeigt Ihnen, welche Datensätze nicht mit den Einträgen in der Systemdatei übereinstimmen. Anschließend wird Ihnen aufgezeigt, wie Sie das Profil mit der Systemdatei abgleichen können. In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

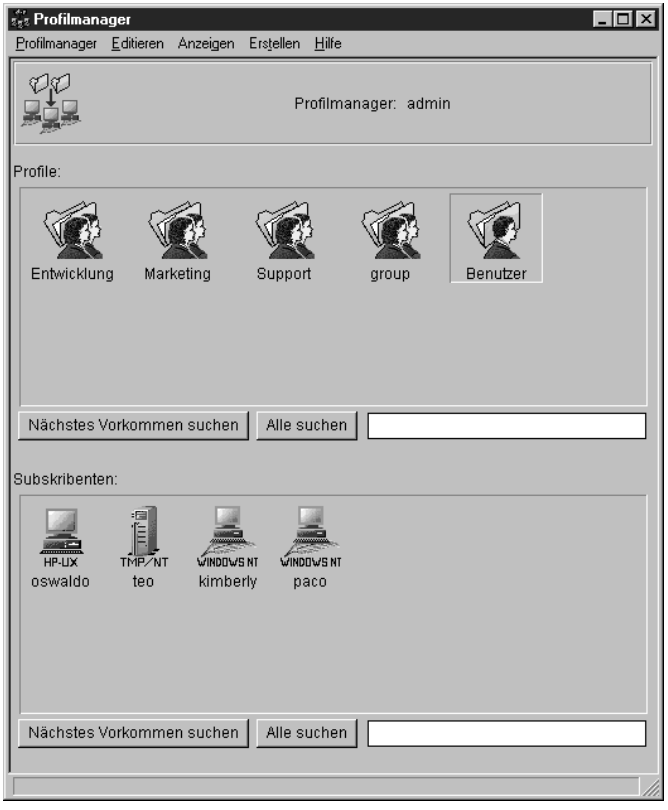
Aktivität	Umgebung	Berechtigungsklasse
Profildatenbank mit Systemdateien synchronisieren	Gruppenprofil	**admin**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um die Profildatenbank mit Systemdateien zu synchronisieren:

1. Klicken Sie in einem Profilmanager doppelt auf das Symbol eines Subskribenten des Profilmanagers, um das Fenster **Profilmanager** anzuzeigen.



2. Wählen Sie **Synchronisieren** im Kontextmenü des Symbols eines verwalteten Knotens aus, um den Dialog **Profile synchronisieren** anzuzeigen.

3. Wählen Sie **GroupProfile** in der Liste **Verfügbare Profilarten** aus.

4. Klicken Sie auf **Synchronisieren**, um die Datenbank mit dem Subskribentensystem zu synchronisieren.

   Tivoli überprüft das Profil und die Subskribentensysteme auf Unterschiede, anschließend zeigt es den Dialog **Profil-/Systemdiskrepanzen** an.

   Der Dialog **Profil-/Systemdiskrepanzen** zeigt die Unterschiede zwischen den Benutzerkonfigurationsdateien auf den Subskribentensystemen und dem aktuellen Profil an. Sie können auf **Änderungen festschreiben** klicken, um die Informationen aus den Systemdateien in das Profil zu kopieren. Sie können aber auch auf **Schließen** klicken und die erforderlichen Änderungen vornehmen, indem Sie dem Profil Einträge manuell hinzufügen oder Einträge manuell daraus löschen.

   Wenn Sie auf **Änderungen festschreiben** klicken, wählen Sie die Option **Speichern** im Menü **Profil** des Fensters **Gruppenprofilmerkmale** aus, um die Änderungen an der Profildatenbank zu speichern.

Anmerkung: Mit einer Synchronisation wird nur die Kopie des Profils des verwalteten Knotens aktualisiert, nicht das Profil der höchsten Ebene.

Befehlszeile

Im folgenden Beispiel werden die Datensätze eines Gruppenprofils mit ihren entsprechenden Einträgen in den Konfigurationsdateien der Subskribentensysteme überprüft:

```
wchkgrps @GroupProfile:developers @ManagedNode:kenya
```

Dabei gilt Folgendes:

GroupProfile:classicgroups
Gibt den Namen des zu überprüfenden Profils an.

@ManagedNode:kenya
Gibt den Namen des zu überprüfenden Systems an.

Befehlsausgabe:

```
Diese Benutzer wurden zwar im System, nicht aber im angegebenen Profil
bzw. in der angegebenen Datenbank gefunden:

Gruppenname           Kennwort         GID      Mitglieder
dgates
jgriffin
rroyer
```

Weitere Informationen hierzu finden Sie in der Beschreibung des Befehls **wchkgrps** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

Datensätze anhand der Profilrichtlinie überprüfen

Sie können die Datensätze in einem Gruppenprofil anhand der für das Profil definierten Richtlinie überprüfen.

Tivoli überprüft automatisch Datensätze anhand der Profilrichtlinie, wenn ein Datensatz hinzugefügt oder geändert wird. Tivoli überprüft allerdings nur die Attribute von Gruppendatensätzen, die der Richtlinie für Gültigkeitsprüfung zugeordnet wurden.

Wenn die Richtlinie für Gültigkeitsprüfung geändert wurde, seit Sie das letzte Mal Datensätze hinzugefügt oder geändert haben, können Sie alle Datensätze des Profils auf einmal überprüfen, um so die Datensätze zu finden, die der neuen Richtlinie nicht entsprechen.

Im folgenden Skript wird beschrieben, wie Sie alle Datensätze des Profils überprüfen, nachdem die Richtlinie für Gültigkeitsprüfung geändert wurde.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

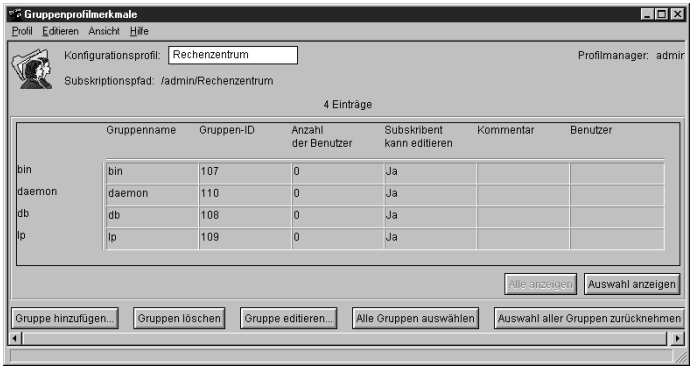
Aktivität	Umgebung	Berechtigungsklasse
Datensätze in Bezug auf die Profilrichtlinien überprüfen	Gruppenprofil	**admin**

Sie können diese Task entweder über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile ausführen.

Arbeitsoberfläche

Führen Sie folgende Schritte aus, um Datensätze anhand der Profilrichtlinie zu überprüfen:

1. Klicken Sie in einem Profilmanager doppelt auf das Symbol eines Gruppenprofils, um das Fenster **Gruppenprofilmerkmale** anzuzeigen.



2. Wählen Sie die Option **Auswerten** im Menü **Profil** aus. Tivoli SecureWay User Administration überprüft die Datensätze im ausgewählten Gruppenprofil und zeigt einen Dialog an, in dem die Datensätze aufgelistet werden, die die Gültigkeitsprüfung nicht bestanden haben.

Ergebnisse der Richtliniengültigkeitsprüfung
Ergebnisse der Richtliniengültigkeitsprüfung für Profil: group in Profilmanager: admin
Alle Datensätze haben die Richtliniengültigkeitsprüfung bestanden.
Verlassen
Hilfe...

Befehlszeile

Im folgenden Beispiel werden Datensätze in einem Gruppenprofil überprüft:

```
wvalidate @GroupProfile:developers
```

Befehlsausgabe:

```
dgates Gültigkeitsprüfung fehlgeschlagen
rroyer Gültigkeitsprüfung fehlgeschlagen
```

Informationen zum Überprüfen eines Gruppendatensatzes über die Befehlszeile finden Sie in der Beschreibung des Befehls **wvalidate** im Handbuch *Tivoli Framework Reference Manual*.

Gruppendatensatz suchen

Es gibt Situationen, in denen Sie ein Profil geöffnet haben und dort eine Gruppe suchen müssen. Tivoli SecureWay User Administration stellt Ihnen ein Tool für die Suche nach Gruppen in einem Profil zur Verfügung.

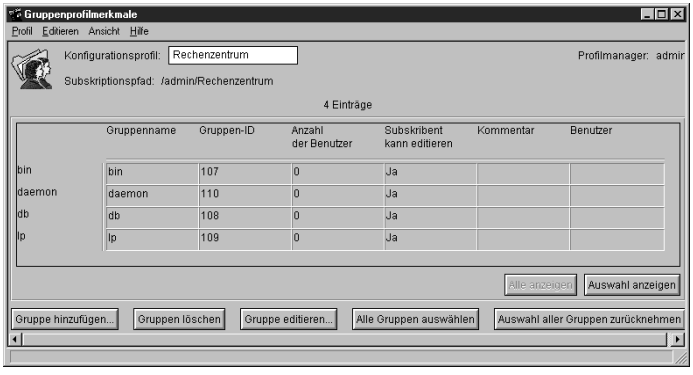
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Gruppendatensatz in einem Gruppenprofil suchen	Gruppenprofil	**user**

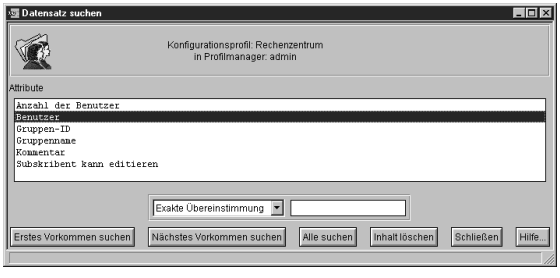
Sie können diese Task nur über die Tivoli-Arbeitsoberfläche ausführen.

Führen Sie folgende Schritte aus, um einen Datensatz in einem Gruppenprofil zu suchen:

1. Klicken Sie im Profilmanager doppelt auf ein Profil, um das Fenster **Gruppenprofilmerkmale** anzuzeigen.



2. Wählen Sie **Suchen** im Menü **Ansicht** aus, um den Dialog **Datensatz suchen** anzuzeigen.



3. Wählen Sie die entsprechenden Attribute in der Liste **Attribute** aus. Diese Attribute werden von Tivoli SecureWay User Administration zur Definition der Suchkriterien verwendet.
4. Wählen Sie eine der folgenden Sucharten aus dem Kontextmenü aus:
   - **Enthält**

     Gibt an, dass die gefundenen Datensätze den Wert des Suchbegriffs enthalten.
   - **Exakte Übereinstimmung**

     Gibt an, dass die gefundenen Datensätze mit dem Suchbegriff exakt übereinstimmen.
   - **Größer als**

     Gibt an, dass der Wert des ausgewählten Attributs für die gefundenen Datensätze größer ist als der Wert des Suchbegriffs.
   - **Kleiner als**

     Gibt an, dass der Wert des ausgewählten Attributs für die gefundenen Datensätze kleiner ist als der Wert des Suchbegriffs.
5. Geben Sie einen Wert für den Suchbegriff ein. Der Suchbegriff für das Attribut kann ein beliebiger gültiger Wert sein.
6. Klicken Sie auf **Erstes Vorkommen suchen**, um das erste Vorkommen eines lokalen Druckdienstes zu suchen, das mit dem Suchbegriff übereinstimmt.

   — ODER —

   Klicken Sie auf **Nächstes Vorkommen suchen**, um das nächste Vorkommen eines lokalen Druckdienstes zu suchen, das mit dem Suchbegriff übereinstimmt.

   — ODER —

   Klicken Sie auf **Alle suchen**, um alle lokalen Druckdienste zu suchen, die mit dem Suchbegriff übereinstimmen.

Von einer Profilkopie in eine andere wechseln

Sie können von einem beliebigen Profil zu einer anderen Kopie des aktuellen Profils in der Subskriptionshierarchie wechseln und diese anzeigen. Abhängig von Ihrer Berechtigungsklasse können Sie für die neu angezeigte Profilkopie Vorgänge ausführen. Dies kann hilfreich sein, wenn Sie ein Profil anzeigen und Änderungen am Profil prüfen oder vornehmen möchten.

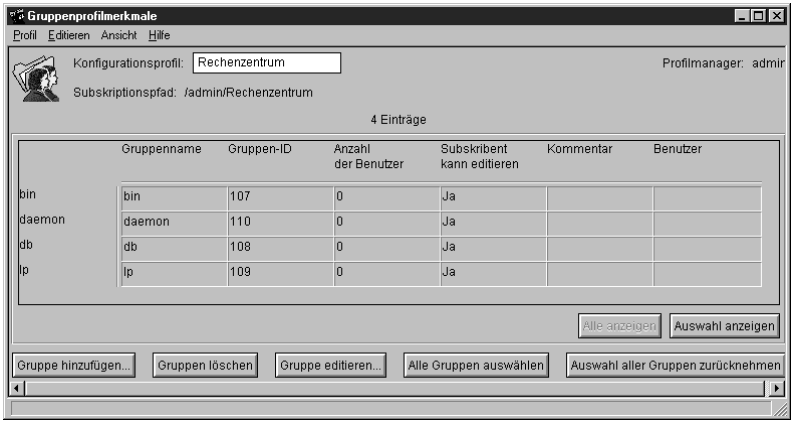
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Von einer Profilkopie in eine andere wechseln	Gruppenprofil	**user**

Sie können diese Task nur über die Tivoli-Arbeitsoberfläche ausführen.

Führen Sie folgende Schritte aus, um zwischen Benutzerprofilkopien zu wechseln:

1. Klicken Sie im Profilmanager doppelt auf ein Profil, um das Fenster **Gruppenprofilmerkmale** anzuzeigen.



2. Wählen Sie **Zu Profil auf** im Menü **Profil** aus, um den Dialog **Zu Profil** anzuzeigen.

3. Wählen Sie den Subskribenten mit der Kopie des anzuzeigenden Profils aus.
4. Wählen Sie die Kopie des anzuzeigenden Profils aus.
5. Klicken Sie auf **Zu... und anzeigen** bzw. **Zu... und editieren**, um die Profilkopie anzuzeigen bzw. zu editieren.

Gruppendatensätze sortieren

Sie können die Reihenfolge festlegen, in der die Gruppendatensätze im Fenster **Gruppenprofilmerkmale** angezeigt werden. Wenn Sie jedoch das Fenster schließen, geht die Sortierung verloren. Wenn Sie das Fenster erneut öffnen, werden die Datensätze in der Standardreihenfolge angezeigt.

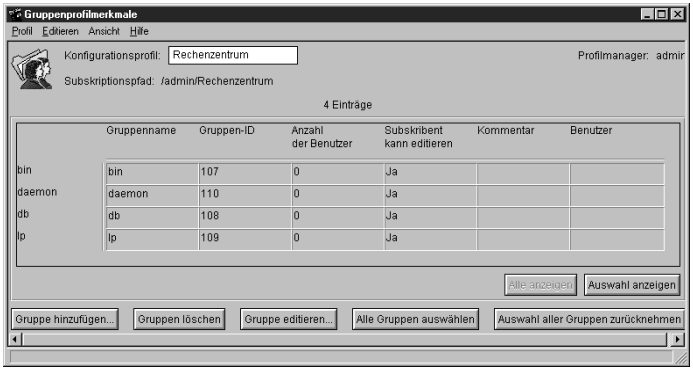
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Gruppendatensätze sortieren	Gruppenprofil	**user**

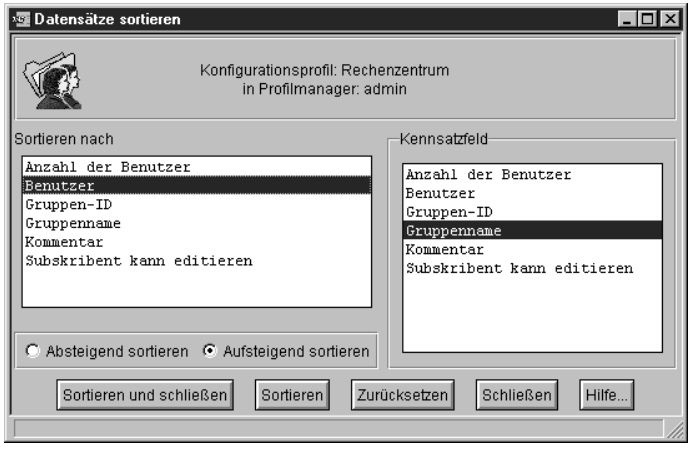
Sie können diese Task nur über die Tivoli-Arbeitsoberfläche ausführen.

Führen Sie folgende Schritte aus, um Gruppendatensätze zu sortieren:

1. Klicken Sie im Profilmanager doppelt auf ein Profil, um das Fenster **Gruppenprofilmerkmale** anzuzeigen.



2. Wählen Sie im Menü **Ansicht** nacheinander **Sortieren –> Gruppen** aus, um den Dialog **Datensätze sortieren** anzuzeigen.



3. Wählen Sie in der Liste **Sortieren nach** das Attribut aus, nach dem sortiert werden soll. Die Datensätze werden nach dem Attribut sortiert, das Sie in der Liste **Sortieren nach** auswählen.

4. Wählen Sie das Attribut aus, dessen Kennung in der linken Spalte des Fensters **Gruppenprofilmerkmale** angezeigt werden soll.

   Sie können in der linken Spalte des Profilfensters die linke Maustaste drücken, um Datensätze auszuwählen. Dies entspricht dem Auswählen eines Datensatzes durch Drücken der Maustaste innerhalb des Tabellenbereichs.

5. Klicken Sie auf **Sortieren und schließen**, um die Datensätze zu sortieren und zum Fenster **Gruppenprofilmerkmale** zurückzukehren.

Gruppendatensatzattribute sortieren

Sie können festlegen, in welcher Reihenfolge die Attribute von Gruppenkontodatensätzen im Fenster **Gruppenprofilmerkmale** angezeigt werden. Wenn Sie jedoch das Fenster schließen, geht die Reihenfolge verloren. Wenn Sie das Fenster erneut öffnen, werden die Datensätze in der Standardreihenfolge angezeigt.

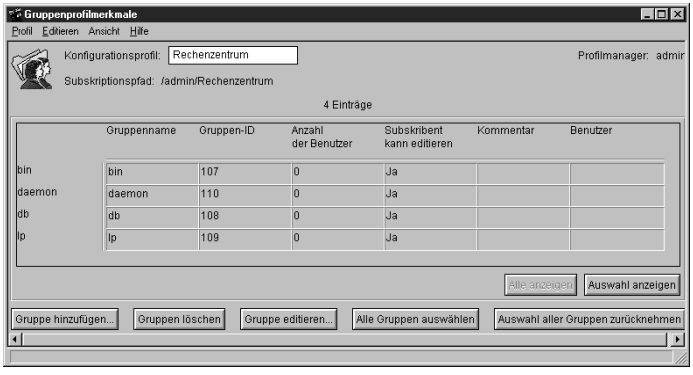
In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Attribute sortieren und anzeigen	Gruppenprofil	**user**

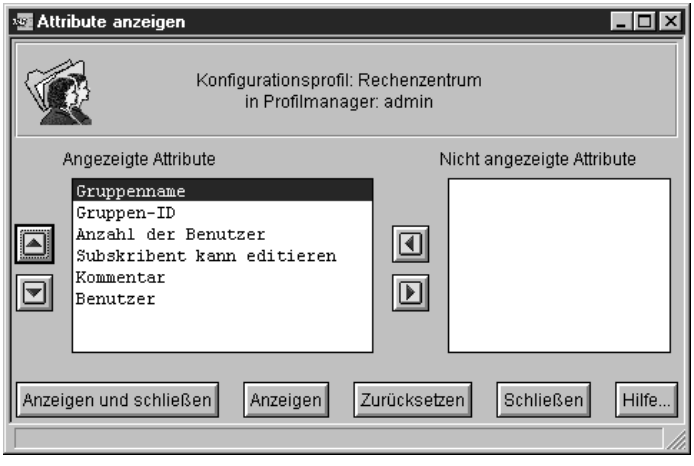
Sie können diese Task nur über die Tivoli-Arbeitsoberfläche ausführen.

Führen Sie folgende Schritte aus, um Gruppendatensatzattribute zu sortieren und anzuzeigen:

1. Klicken Sie im Profilmanager doppelt auf ein Profil, um das Fenster **Gruppenprofilmerkmale** anzuzeigen.



2. Wählen Sie im Menü **Ansicht** nacheinander **Sortieren –> Attribute** aus, um den Dialog **Attribute anzeigen** aufzurufen.



3. Wählen Sie die Attribute aus, die in der Liste **Angezeigte Attribute** nicht angezeigt werden sollen. Klicken Sie auf den Rechtspfeil, um das ausgewählte Attribut in die Liste **Nicht angezeigte Attribute** zu verschieben.

4. Wählen Sie ein Attribut in der Liste **Angezeigte Attribute** aus, und klicken Sie auf den Aufwärtspfeil oder den Abwärtspfeil, um es an die Position zu verschieben, an der das Attribut im Fenster **Gruppenprofilmerkmale** angezeigt werden soll.

   Wiederholen Sie diesen Schritt, bis alle Attribute in der gewünschten Reihenfolge aufgelistet werden.

5. Klicken Sie auf **Anzeigen und schließen**, um die Datensätze zu sortieren und zum Fenster **Gruppenprofilmerkmale** zurückzukehren.

10

Prüfprotokollierung

Tivoli SecureWay User Administration unterstützt mit Hilfe der folgenden Befehle die Prüfprotokollierung. Somit können Sie alle Aktivitäten, bei denen Daten auf dem TMR-Server geändert werden, prüfen und aufzeichnen.

- Befehl **wusraudit**
- Befehl **wusrauditqry**

Mit dem Befehl **wusraudit** aktivieren Sie die Steuerkomponente für die Prüfprotokollierung auf dem TMR-Server. Diese Steuerkomponente überwacht alle von Tivoli SecureWay User Administration-Operationen ausgelösten Aktivitäten, wie z. B. Erstellen, Löschen, Füllen, Verteilen, Kopieren, Zusammenfügen usw. Diese Aktivitäten werden als Prüfdatensätze protokolliert. Diese bestehen aus einem Standard-Header mit einem festgelegten Format sowie einer Liste mit durch Komma voneinander abgetrennten Paarungen aus Namen und Werten. Das einfache Format dieser Liste ermöglicht den Import in Tabellenkalkulationsprogramme und Datenbanken sowie die direkte Anzeige am Bildschirm.

Zusätzlich können Sie mit dem Befehl **wusraudit** den Namen, den Standort und die Größe der Prüfprotokolldatei angeben. Außerdem können Sie festlegen, ob beim Überschreiten der maximalen Größe eine Kopie der Datei archiviert werden soll und ob die Protokollausgabe zwischengespeichert werden soll, bevor sie in die Prüfprotokolldatei geschrieben wird.

Mit dem Befehl **wusrauditqry** können Sie jederzeit eine Liste der derzeit aktiven Parameter auf dem Bildschirm anzeigen. Falls Parameter geändert werden sollen, können Sie mit dem Befehl **wusraudit** die Prüfung stoppen und mit den geänderten Parametern erneut starten.

Anmerkung: Für die Ausführung der Prüfprotokollbefehle ist die Berechtigungsklasse **admin** erforderlich. Auf UNIX-Systemen ist **root** der Besitzer der Prüfprotokolldatei. Nur er verfügt über Lese- und Schreibzugriffsrechte. Auf NT-Systemen verfügt die Gruppe der lokalen Administratoren des TMR-Servers über uneingeschränkten Zugriff auf die Prüfprotokolldatei. Der lokale Benutzer **tmersvrd** des TMR-Servers verfügt über Schreibzugriffsrechte. Das Verzeichnis mit der Prüfprotokolldatei verfügt nur über die Schutzmechanismen, die vom Systemadministrator als notwendig erachtet werden.

In diesem Kapitel werden folgende Themen beschrieben:

- Prüfprotokollierung aktivieren
- Aktive Parameter ermitteln
- Stoppen und mit geänderten Parametern neu starten
- Format des Prüfprotokolls
- Protokollierte Operationen von Tivoli SecureWay User Administration

Steuerkomponente für die Prüfprotokollierung aktivieren

Mit dem Befehl **wusraudit** aktivieren Sie die Steuerkomponente für die Prüfprotokollierung, die sich auf dem TMR-Server befindet. Außerdem geben Sie mit dem Befehl die Prüfprotokollparameter an.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Prüfprotokollierung aktivieren	TMR	**admin**

Sie können diese Task nur über die Befehlszeile ausführen.

Im folgenden Beispiel werden die Steuerkomponente für die Protokollierung aktiviert sowie der Name und die maximale Größe der Prüfprotokolldatei angegeben:

```
wusraudit -l 1 -f /server/directory/audit.log -s 2
```

Dabei gilt Folgendes:

-l 1
Aktiviert die Steuerkomponente für die Prüfprotokollierung.

-f /server/directory/audit.log
Gibt den vollständigen Pfad der Prüfprotokolldatei an.

-s 2
Gibt an, dass die maximale Größe der Prüfprotokolldatei 2 MB beträgt.

Sie können auch angeben, ob die Prüfprotokolldatei beim Erreichen der maximalen Größe archiviert oder gelöscht werden soll. Außerdem können Sie angeben, ob die Prüfprotokolldatensätze zunächst zwischengespeichert oder direkt in die Prüfprotokolldatei geschrieben werden sollen. Verwenden Sie hierzu folgende Parameter:

-a ENABLED gibt an, dass die Prüfprotokolldatei archiviert werden soll. DISABLED gibt an, dass die Prüfprotokolldatei beim Erreichen der maximalen Größe gelöscht werden soll. Standardeinstellung ist ENABLED.

-b ENABLED gibt an, dass mehrere Datensätze zwischengespeichert werden sollen, bevor sie in die Prüfprotokolldatei geschrieben werden. DISABLED gibt an, dass jeder Datensatz sofort in die Prüfprotokolldatei geschrieben werden soll. Standardeinstellung ist ENABLED.

Anmerkung: In den meisten Fällen sollten Sie ENABLED auswählen, um die Systemleistung zu verbessern. Sollen jedoch höchste Sicherheitsstandards eingehalten werden, wählen Sie DISABLED aus, um zu verhindern, dass Datensätze in einem Puffer zwischengespeichert werden.

Aktive Parameter ermitteln

Mit dem Befehl **wusrauditqry** können Sie eine Liste der derzeit aktiven Parameter auf dem Bildschirm anzeigen.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Prüfprotokollparameter ermitteln	TMR	**admin**

Sie können diese Task nur über die Befehlszeile ausführen.

Im folgenden Beispiel werden die aktiven Prüfprotokollparameter auf dem Bildschirm angezeigt:

```
wusrauditqry
```

Nachfolgend ein Beispiel für die Ausgabe von **wusrauditqry**:

```
User Administration-Prüfprotokollierung ist aktiviert.
Aktuelle Werte von Prüfprotokollparametern:
   Prüfprotokollierungsstufe
   Prüfprotokolldateipfad:  /data/audit/nb.audit
   Maximale Größe der Prüfprotokolldatei (MB):  1
   Archivierung der Prüfprotokolldateien ist ENABLED
   Pufferung mehrerer Prüfprotokolldatensätze ist ENABLED
```

Stoppen und mit geänderten Parametern erneut starten

Mit dem Befehl **wusraudit** können Sie die Steuerkomponente für die Prüfprotokollierung stoppen. Es wird empfohlen, die Steuerkomponente für die Prüfprotokollierung nicht nur zum Ändern von Parametern, sondern auch in den folgenden Fällen zu stoppen:

- Wenn der Befehl **wchkadmdb** verwendet werden soll.
- Wenn der Befehl **wchkusers** verwendet werden soll.
- Wenn die Datenbank wiederhergestellt werden soll.
- Wenn eine Aktualisierung auf ein neues Release durchgeführt werden soll.

All diese Aktivitäten lösen eine große Anzahl Prozesse aus, so dass bei aktiver Prüfprotokollierung und Archivierungeine große Menge an Plattenspeicherplatz erforderlich ist.

In der folgenden Tabelle werden die Umgebung und die Berechtigungsklasse, die für diese Task erforderlich sind, aufgeführt:

Aktivität	Umgebung	Berechtigungsklasse
Prüfprotokollierung stoppen	TMR	**admin**

Sie können diese Task nur über die Befehlszeile ausführen.

Im folgenden Beispiel wird die Steuerkomponente für die Prüfprotokollierung gestoppt:

```
wusraudit -l 0
```

Nachdem Sie die Steuerkomponente für die Prüfprotokollierung gestoppt haben, können Sie sie mit den neuen Parametern erneut starten.

Im folgenden Beispiel werden die Steuerkomponente für die Prüfprotokollierung erneut gestartet, die maximale Größe der Prüfprotokoll-

datei festgesetzt und die Archivierung der Datei sowie die Zwischenspeicherung von Protokollnachrichten inaktiviert:

```
wusraudit -l 1 -f /server/directory/audit.log -s4 -a DISABLED -b DISABLED
```

Dabei gilt Folgendes:

-l 1
Aktiviert die Steuerkomponente für die Prüfprotokollierung.

-f /server/directory/audit.log
Gibt den vollständigen Pfad der Prüfprotokolldatei an.

-s 4
Gibt an, dass die maximale Größe der Prüfprotokolldatei 4 MB beträgt.

-a DISABLED
Gibt an, dass die Prüfprotokolldatei beim Erreichen der maximalen Größe gelöscht wird.

-b DISABLED
Gibt an, dass jeder Prüfdatensatz sofort in die Prüfprotokolldatei geschrieben wird.

Format des Prüfprotokolls

Alle Prüfprotokolldatensätze beginnen mit einem Standard-Header im festgelegten Format.

Nachfolgend ein Beispiel für einen solchen Header:

18355_1383392,05/15/2001 11:29:24,
1,root@hummer.austin.na.tivoli.com,CLI,″wusrauditqry″

Dabei gilt Folgendes:

18355_1383392
Gibt die eindeutige Prozess-ID (18355) und die Thread-ID (1383392) der Operation an.

05/15/2001 11:29:24
Gibt das Datum und die Zeitmarke der Operation an.

1 Gibt an, dass die Steuerkomponente für die Prüfprotokollierung aktiv ist.

root@hummer.austin.na.tivoli.com
Gibt die Anmelde-ID des Administrators an, der die Operation aufgerufen hat.

CLI
Gibt an, dass die Operation von der Befehlszeile aus aufgerufen wurde.

wusrauditqry
Gibt die aufgerufene Operation an.

Bei den meisten Prüfprotokolldatensätzen folgen auf den Standard-Header mit festgelegtem Format Paarungen aus Name und Wert, die durch Kommata voneinander getrennt sind. Durch diese einfache Formatierung wird der Import in Tabellenkalkulationsprogramme und Datenbankanwendungen sowie die Anzeige in einem Texteditor wie z. B. Notepad ermöglicht.

Nachfolgend ein Beispielausschnitt aus einem Prüfprotokolldatensatz mit Paarungen aus Name und Wert:

```
18711_1915648,05/15/2001
13:19:53,1,root@hummer.austin.na.tivoli.com,from
add_records(),entry_flags=65544,real_name=″Ray
Lachance″,login_name=″pio″,password=″***″,
passwd_aging=DISABLED,...
```

Diese Paarungen werden innerhalb der Prüfprotokolldatensätze durch Kommata voneinander getrennt. Die Daten sind von der jeweiligen Operation abhängig. So steht z. B. `real_name="Ray Lachance"` für den Namen eines Benutzers, für den ein Datensatz hinzugefügt wird.

Die Formatierung der Werte in den Prüfprotokolldatensätzen folgt folgender Struktur:

- Zeichenfolgen werden in Anführungszeichen gesetzt. Der Attributwert `Horace` wird z. B. folgendermaßen formatiert: `"Horace"`.

  Enthält eine Zeichenfolge Anführungszeichen, werden diese im Prüfprotokolldatensatz verdoppelt. So wird z. B. die Zeichenfolge `Owner of the "smart" brand` folgendermaßen formatiert `"Owner of the ""smart"" brand"`.

  Enthält eine Zeichenfolge einen Ausdruck in eckigen Klammern, werden diese im Prüfprotokolldatensatz verdoppelt. Die Zeichenfolge `Department 12<bldg1>` wird z. B. folgendermaßen formatiert: `"Department 12<<bldg1>>"`.

- Bei Zeichenfolgenlisten handelt es sich um Attribute, die über mehr als einen Wert verfügen und aus mindestens einer Zeichenfolge bestehen. Die Zeichenfolgenlisten werden im Prüfprotokolldatensatz in Anführungszeichen gesetzt. Die einzelnen Zeichenfolgenelemente, aus der sicht die Zeichenfolgenliste zusammensetzt, werden in folgende Zeichen gesetzt: <>.

  Die Zeichenfolgenliste

  ```
  Machine A   Machine B   Machine C
  ```

  wird z. B. folgendermaßen formatiert:

  ```
  "<Machine A><Machine B><Machine C>"
  ```

  Anführungszeichen und eckige Klammern innerhalb einer Zeichenfolgenliste werden im Prüfprotokolldatensatz verdoppelt (wie auch bei einfachen Zeichenfolgen).

- Numerische Werte werden nicht in Anführungszeichen gesetzt. Der Attributwert `304` wird z. B. folgendermaßen formatiert: `304 .`

- Boolesche Werte werden im Prüfprotokolldatensatz entweder als `ENABLED` oder als `DISABLED` angezeigt.

- Kennwörter werden wie folgt dargestellt: `"***"` .
- Das Datum wird im länderspezifischen Format dargestellt. So erscheint das Datum 15. Mai 2001 in einem deutschen System im Format `15/05/2001`, in einem US-amerikanischen System hingegen im Format `05/15/2001`.
- Oktettlisten werden als Listen mit hexadezimalen Werten formatiert. Der Oktettwert `00000001 11111100 11100000` wird z. B. folgendermaßen formatiert: `X'01FCE0'`.

Protokollierte Operationen von Tivoli SecureWay User Administration

Folgende Operationen von Tivoli SecureWay User Administration werden geprüft und protokolliert:

- Benutzerdatensatzbefehle
  - wcpusr
  - wcrtusr
  - wdelusr
  - wgenusrdef
  - wgetusr
  - wlsusrs
  - wmrgusrs
  - wmvusr
  - wsetusr
  - wsetusrs
- Kennwortbefehle
  - wpasswd
  - wpasswdsync

- Benutzerprofilbefehle
  - wpopusrs
  - wchkusrs
- Verschiedene Befehle
  - wutshacts
  - wmodals
  - wupdhdir
  - wsetnds
  - wrunusrcmd
  - wsetusrcfg
  - wusrdbrep
  - wusraudit
  - wusrauditqry

11

Tivoli SecureWay User Administration anpassen

In diesem Kapitel wird die Anpassung von Tivoli SecureWay User Administration mit Hilfe von Tivoli AEF (Application Extension Facility) erläutert. Bevor Sie Anpassungen vornehmen, sollten Sie sich zunächst mit den Informationen im Handbuch *Tivoli AEF User's Guide* vertraut machen.

Tivoli AEF bietet Ihnen die Möglichkeit, Profilen Attribute hinzuzufügen. Der Schwerpunkt in diesem Kapitel liegt auf der Anpassung der Benutzer- und Gruppenkomponenten von Tivoli SecureWay User Administration.

Profilbasierte Anwendungen, wie zum Beispiel Tivoli SecureWay User Administration, unterstützen die folgenden Grafikobjekte, um Attribute von Tivoli AEF auf der Arbeitsoberfläche zu bearbeiten:

- Auswahlgrafikobjekt
- Textgrafikobjekt
- Seitengrafikobjekt
- Schaltergrafikobjekt

Anpassungsstrategie

Tivoli AEF ermöglicht Folgendes:

- Merkmale definieren, um Daten zu verwalten, die Tivoli SecureWay User Administration momentan nicht verwaltet
- Aktionen definieren, die ein Skript oder ein Programm während der Verteilung eines Profils ausführen
- Werte für neue Merkmale (über CLI-Befehle) zurückgeben oder setzen
- Benutzerschnittstelle anpassen, um den Zugriff auf neue Merkmale zu erteilen, die Gruppe der Attribute zu begrenzen, auf welche ein Administrator Zugriff hat, oder den Zugriff auf eine weitere Anpassung zu erteilen

Die Definition neuer Merkmale und Aktionen sowie die Anpassung des Zugriffs auf Merkmale (mit CLI-Befehlen) stellt keinen tiefen Eingriff dar und kann leicht beibehalten werden. Das Anpassen der Benutzerschnittstelle kann jedoch zu Problemen bei der Aktualisierung führen.

Die Anpassung eines vorhandenen Dialogs von Tivoli SecureWay User Administration bedeutete normalerweise, dass der gesamte Dialog ersetzt wurde. Obwohl diese Vorgehensweise sehr leistungsfähig war und eine große Flexibilität bot, entstanden dadurch folgende Probleme:

- Der Benutzer musste einen ganzen Dialog korrekt ersetzen, ohne die Funktionalität von Tivoli SecureWay User Administration zu stören.
- Aktualisierungen unter Beibehaltung der Anpassungen wurden erschwert, wenn nicht unmöglich gemacht, da Aktualisierungen Anpassungen nicht erkennen.

Damit Anpassungen der Benutzerschnittstellen leichter verwaltet und erweitert werden können, verfügt Tivoli SecureWay User Administration jetzt über eine Anpassungsstrategie für Benutzerschnittstellen. Statt einen ganzen Dialog zu ersetzen, können Sie jetzt eine Reihe von CLI-Befehlen verwenden, um Ihren eigenen Dialog für Tivoli SecureWay User Administration hinzuzufügen.

Anmerkung: Das Hinzufügen von benutzerdefinierten Attributen zu Tivoli-Anzeigen bzw. von Tivoli-Attributen zu benutzerdefinierten Anzeigen sollte nach Möglichkeit vermieden werden. Jede Tivoli-Anzeige enthält prozeduralen Code. Daher haben Änderungen an der DSL-Datei (Dialog Specification Language) einer Tivoli-Anzeige nicht unbedingt das gewünschte Resultat. In einigen Fällen können solche Änderungen zu Laufzeitfehlern führen. Informationen zu DSL-Dateien finden Sie im Handbuch *Tivoli AEF User's Guide*.

Die Dialoge für die Verwaltung von Benutzern und Gruppen werden in drei Komponenten unterteilt: Kategorien, Unterkategorien und Anzeigen.

Kategorien der Benutzer- und Gruppenverwaltung

Benutzerattribute werden in Kategorien unterteilt. Die Kategorien decken die folgenden Hauptthemen der Benutzerinformationen ab:

- Allgemeine Benutzerinformationen (**General**)
- UNIX-Benutzerinformationen (**UNIX**)
- Windows NT-Benutzerinformationen (**Windows NT**)
- NetWare-Benutzerinformationen (**NetWare**)

Mit dem Befehl **wcrtusrcat** können Sie neue Kategorien erstellen. Mit diesem Befehl können Sie angepasste Kategorien erstellen, die Ihren Anforderungen genügen.

Unterkategorien der Benutzer- und Gruppenverwaltung

Jedes Hauptthema der Benutzerinformationen enthält mehrere Gruppen von zusammengehörigen Attributen oder Unterkategorien. Die folgenden Beispiele von Unterkategorien werden momentan in Tivoli SecureWay User Administration unterstützt:

- Allgemeine Informationen zur Benutzeridentifikation (**Kennung**)
- Informationen zur Windows NT-Anmeldung (**Windows NT-Anmeldung**)
- Informationen zum NetWare-Kennwort (**NetWare-Kennwort**)
- Informationen zum UNIX-Basisverzeichnis (**UNIX-Verzeichnis**)

Mit dem Befehl **wcrtusrsubcat** können Sie neue Unterkategorien erstellen. Mit diesem Befehl können Sie angepasste Unterkategorien für neue oder vorhandene Kategorien erstellen.

Darüber hinaus können Sie mit dem Befehl **wcrtusrsubcat** von Ihnen erstellte Unterkategorien ändern.

Anzeigen der Benutzer- und Gruppenverwaltung

Jede Unterkategorie der Benutzer- und Gruppenverwaltung entspricht einer anzeigbaren Dialoganzeige, das heißt, dass es eine 1:1-Entsprechung von Dialoganzeige und Unterkategorie gibt. Jede Anzeige enthält Attribute, die der Unterkategorie zugeordnet sind. Der der Unterkategorie **Windows NT-Anmeldung** zugeordnete Bereich enthält momentan zum Beispiel folgende Attribute:

- **Anmeldung aktivieren**
- **Anmeldename**
- **Benutzer-ID**
- **Kontoart**
- **Anmeldeskript**

Der Befehl **wcrtusrsubcat** ordnet der neuen Anzeige eine neue Unterkategorie zu. Mit diesem Befehl können Sie angepasste Anzeigen erstellen, die bei Auswahl einer benutzerdefinierten Unterkategorie angezeigt werden.

Diese neuen Anzeigen sollten in DSL geschrieben sein und dem Darstellungsobjekt mit dem Befehl **wputdialog** hinzugefügt werden. Der Hauptunterschied zwischen dem Hinzufügen einer angepassten Anzeige und dem Ersetzen eines ganzen Dialogs besteht darin, dass die Anpassungen separat vom Tivoli SecureWay User Administration-Dialog gespeichert und beim Öffnen des Dialogs dynamisch geladen werden.

Diese Strategie schafft eine Grenze zwischen der Anwendung Tivoli SecureWay User Administration und den Anpassungen; dadurch können die Anpassungen bei Aktualisierungen von Tivoli SecureWay User Administration beibehalten werden.

Kategorien und Unterkategorien löschen

Sie können nicht nur neue Kategorien und Unterkategorien hinzufügen, sondern diese auch löschen. Mit dem Befehl **wdelusrcat** werden benutzerdefinierte Kategorien gelöscht und die von Tivoli SecureWay User Administration bereitgestellten Kategorien und Unterkategorien verdeckt. Wenn Sie zum Beispiel die Kategorie **Windows NT** löschen, zeigt Tivoli SecureWay User Administration die Windows NT-Unterkategorien nicht an.

Die Befehle **wlsusrcat** und **wlsusrsubcat** listen Kategorien und Unterkategorien auf. Mit dem Befehl **wdelusrsubcat** werden benutzerdefinierte Unterkategorien gelöscht und von Tivoli SecureWay User Administration bereitgestellte Unterkategorien verdeckt. Diese Befehle werden wie folgt verwendet:

- Um eine verdeckte, von Tivoli SecureWay User Administration zur Verfügung gestellte Kategorie und deren Unterkategorien wieder anzuzeigen, erstellen Sie die Kategorie mit dem Befehl **wcrtusrcat** erneut.
- Um eine verdeckte, von Tivoli SecureWay User Administration zur Verfügung gestellte Unterkategorie wieder anzuzeigen, erstellen Sie die Unterkategorie mit dem Befehl **wcrtusrsubcat** erneut.

Beispiel einer Dialoganpassung

In den folgenden Abschnitten wird erläutert, wie die Unterkategorie **Security** der Kategorie **General** hinzugefügt wird.

Anmerkung: Sie müssen für dieses Beispiel AEF installiert haben.

Die Anzeige, die der Unterkategorie **Security** zugeordnet ist, enthält die neuen Attribute **ssn** und **badge**.

Einem Profil neue Attribute hinzufügen

Wenn Sie einem Profil neue Attribute hinzufügen möchten, verwenden Sie den Befehl **waddprop**. Dieser Befehl fügt ein neues Attribut nur dem angegebenen Profil hinzu; das Attribut wird an beliebige Profilkopien weitergegeben, wenn Sie das Profil verteilen. Da dieses Attribut auch in einigen Dialogen erscheinen muss (wie zum Beispiel den Dialogen zum Hinzufügen, Editieren und Anzeigen), gibt es einige Namenskonventionen, die Sie beachten müssen.

- Der Attributname muss innerhalb eines Profils eindeutig sein.
- Das Attribut wird als Spaltenüberschrift in der Tabelle für den angegebenen Profilmerkmaledialog verwendet. Daher sollten Sie einen Namen auswählen, der Aufschluss über die Verwendung des Attributs gibt. Sie können Leerzeichen in einem Attributnamen mit Unterstrichen (_) wiedergeben, zum Beispiel **neuer_Standort**.
- Es sind nur die folgenden Zeichen zulässig: [(a-z), (A-Z), (0-9),"-", "_"]
- Dem Attribut darf nur ein Zeichenfolgewert zugeordnet sein. Skripts und Konstanten sind ungültig.

Im folgenden Beispiel wird einem Benutzerprofil ein neues Attribut hinzugefügt:

1. Rufen Sie den vollständigen Namen des Benutzerprofils ab, das Sie verwenden möchten. Geben Sie Folgendes in der Befehlszeile ein, um eine Liste mit allen verfügbaren Benutzerprofilen abzurufen:

```
> wlookup -r UserProfile -a
marketers      777777.1.515#UserProfile#
developers      777777.1.514#UserProfile#
support         777777.1.517#UserProfile#
sales           777777.1.516#UserProfile#
```

   Anmerkung: Geben Sie den folgenden Befehl ein, um Benutzerattribute aufzulisten:

```
wlspolm -d @UserProfile:ProfileName
```

2. Sie können einem Benutzerprofil wie beispielsweise **developers** die Attribute **ssn** und **badge** wie folgt hinzufügen:

```
> waddprop @UserProfile:developers ssn " "
> waddprop @UserProfile:developers badge " "
```

Anmerkung: Wenn Sie das neu hinzugefügte Attribut entfernen müssen, geben Sie folgenden Befehl ein:

```
> wrmprop @UserProfile:developers ssn
> wrmprop @UserProfile:developers badge
```

3. Sie können die Standardwertegruppe für das neue Attribut zurücksetzen, indem Sie die grafische Benutzerschnittstelle oder den folgenden CLI-Befehl verwenden:

```
> wputpol -d -c 00000\
@UserProfile:developers badge
```

Mit diesem Befehl wird für alle neu im Profil **developers** erstellten Datensätze der Standardwert im Feld **badge** auf **00000** gesetzt. Sie haben nun ein Benutzerprofil **developers** mit den zwei Tivoli AEF-Attributen **ssn** und **badge** und einem Anfangswert sowie einem Standardwert innerhalb der Standardwertegruppe. Wenn Sie das Benutzerprofil **developers** öffnen, können Sie die neue Spalte in der Tabelle sehen.

Profildialog ändern

Nachdem Sie die neuen Attribute hinzugefügt haben, müssen Sie die grafische Benutzerschnittstelle ändern, um diese Felder den Benutzern anzuzeigen. Gehen Sie wie folgt vor:

1. Erstellen Sie die DSL-Datei, in der die Anzeige definiert wird, die der neuen Unterkategorie zugeordnet ist. Um beispielsweise die Datei **/tmp/Security.dsl** zu erstellen, müssen Sie Folgendes eingeben:

```
Partial Dialog {
    Group {
    Name = Security;
    Title = "Security";
        TitlePos = TOP;
    Border = YES;
    ChildColumnAlignment = STRETCH;
      ChildRowAlignment = STRETCH;
    Visible = NO;
```

```
    GridVertical = 0;
    GridHorizontal = 0;

    Group {
      Name = SecurityContainerGroup;
      Layout = VERTICAL;
        ChildColumnAlignment = LEFT;
      ChildRowAlignment = STRETCH;

      Text {
        Name =ssn;
        Title = "Social Security Number";
        TitlePos = TOP;
        ChildColumnAlignment = LEFT;
        ChildRowAlignment = CENTER;
      }
      Text {
        Name = badge;
        Title = "Badge";
        TitlePos = TOP;
        ChildColumnAlignment = LEFT;
        ChildRowAlignment = CENTER;
      }
    } /* SecurityContainerGroup */
  } /*Security*/
} /* partial dialog*/
```

Anmerkung: Die zwei Textgrafikobjekte haben dieselben Namen, **ssn** und **badge**, für die neuen Attribute wie die mit dem Befehl **waddprop** erstellten Attribute.

2. Erstellen Sie die Unterkategorie **Security**, die der Kategorie **General** zugeordnet ist.

   ```
   wcrtusrsubcat –m Security –c General Security
   ```

   Im obigen Befehlsbeispiel wird die Unterkategorie **Security** erstellt und der Kategorie **General** und der DSL-Datei **Security** zugeordnet.

3. Kompilieren Sie den DSL-Code. Beispiel:

   ```
   dsl /tmp/Security.dsl > /tmp/Security.d
   ```

4. Fügen Sie den neuen Dialog in die Darstellungsressource ein. Beispiel:

   ```
   wputdialog -r UserGui Security < /tmp/Security.d
   ```

   Um den kompilierten Dialog **Security.d** der Unterkategorie **Security** zuzuordnen, wenn Sie neue Kategorien oder Unterkategorien hinzufügen, verwenden Sie immer die Darstellungsressource **UserGui**.

12

Weitere Themen

Die hier behandelten Themen sind nicht für alle Benutzer gedacht. In den folgenden Abschnitten werden bestimmte interne Funktionen von Tivoli SecureWay User Administration und der unterstützenden Framework-Komponenten erläutert. Folgende Themen werden behandelt:

- Produktgeschichte
- CCMS, der Anwendungsdienst und Mechanismus zur Datenspeicherung, wird von Tivoli Framework zur Unterstützung von auf Profilen basierenden Anwendungen zur Verfügung gestellt.
- AEF-Aktionen. Hierbei handelt es sich um Skripts, die während einer Profilverteilung ausgeführt werden.
- Sonderverarbeitung von Kennwörtern und zugehörigen Attributen
- Steuerungsdatenfluss zwischen Tivoli Framework und Tivoli SecureWay User Administration während der Verteilung von Benutzerprofilen
- Die verschiedenen Optionen für die Verteilung von Benutzerprofilen, deren Auswirkungen auf Benutzerkonten und -kennwörter sowie die Änderung von Datensätzen auf den Endpunkten
- Benutzer- und Gruppen-Indexdatenbanken und wchkadmdb (Dienstprogramm zur Kundenunterstützung).
- Standardwertegruppendatensatz und die Befehle **waddusrprop**, **waddprop**, **wgenusrdef**

Welche Themen sollten Sie lesen? Wenn Sie ein Systemadministrator sind, der für die Ausführung von Operationen zuständig ist, sollten Sie die Abschnitte zur Verteilung des Benutzerprofils und zur Sonderverarbeitung von Kennwörtern lesen. Wenn Probleme auftreten und die Tivoli-Kundenunterstützung die Verwendung des Befehls **wchkadmdb** empfiehlt, sollten Sie den betreffenden Abschnitt lesen. Wenn Sie für die Entwicklung, Implementierung bzw. den Einsatz zuständig sind, sollten Sie alle Abschnitte lesen.

Produktgeschichte

Tivoli SecureWay User Administration war das ursprüngliche Tivoli-Produkt. Hierbei handelte es sich um ein UNIX-Systemverwaltungs-Tool zur zentralen Verwaltung von Benutzerkonten und -gruppen in verschiedenen UNIX-Implementierungen. Im ursprünglichen Produkt wurde jedes einzelne Benutzerobjekt durch einen Lebkuchenmann dargestellt. Dem System wurde ein Benutzer hinzugefügt, indem der Lebkuchenmann auf das Hostsymbol gezogen wurde. Dieser Ansatz war deutlich besser als frühere Methoden, jedoch stellte die Skalierbarkeit immer noch ein Problem dar.

In Tivoli Management Enterprise 2.0 wurde das System zur Konfiguration und Änderungsverwaltung (CCMS = Configuration and Change Management System) als Plattformebene mit Anwendungsdiensten implementiert. CCMS machte die im ursprünglichen Produkt implementierten Dienste allgemein zugänglich, so dass diese auch von anderen Anwendungen verwendet werden konnten. Darüber hinaus wurden dem Produkt Profile und Profilmanager hinzugefügt. Nun wurden die Benutzerkonten nicht mehr als einzelne Objekte durch Symbole dargestellt, sondern als Datensätze in einem Profil. Ein Profil konnte eine beliebige Anzahl von Datensätzen enthalten, und allen Datensätzen wurden dieselben Standardwertegruppen und Richtlinien für Gültigkeitsprüfung zugeordnet. Einem Profilmanager konnte eine beliebige Anzahl von Profilen und Subskribenten zugeordnet werden. Die verwalteten Knoten oder andere verwaltete Objekte, die von der CCMS-Profilendpunktklasse übernommen wurden, waren Subskribenten, an die Profildaten verteilt wurden und die Profildaten weitergeben konnten.

Tivoli SecureWay User Administration Version 3.0 unterstützte erstmals Windows NT und NetWare über Proxys mit Hilfe der Ressourcenklasse 'PcManagedNode', die vom CCMS-Profilendpunkt übernommen wurde. Mit Version 3.6 stellte Management Framework eine dreistufige Architektur zur Verfügung, die die Tivoli SecureWay User Administration-Unterstützung für Windows NT und NetWare durch die Verwendung eines TMA-Endpunktprozesses, der mit dem TMR-Server über einen Gateway kommunizierte, ermöglichte. Tivoli SecureWay User Administration Version 3.6.2 unterstützte erstmals UNIX-TMA-Endpunkte, LDAP-Verbindungen, OS/2, AS/400, OS/390 in RACF-Umgebungen und GSO. Tivoli SecureWay User Administration Version 3.7 unterstützte erstmals Windows 2000, RedHat Linux und Tivoli SecureWay Policy Director. Andere Unterstützungsfunktionen für Endpunkte wurden von Partnern und Modulherstellern bereitgestellt.

CCMS-Komponenten und -Prozesse

Mit Hilfe von CCMS, einem wesentlichen Tivoli Framework-Dienst, können Anwendungsdaten verwaltet und die Daten über ein hierarisches Subskriptionsmodell an Endpunktagenten verteilt werden. Eine Subskriptionsbeziehung wird erstellt, indem ein Endpunkt einer Objektgruppe, die Daten enthält, als Subskribent zugeordnet wird. Wenn Objektgruppen einander als Subskribenten zugeordnet werden, bilden sie eine Subskriptionsbaumstruktur. Die Objektgruppe zur Verwaltung der CCMS-Subskriptionsbeziehung wird als *Profilmanager* bezeichnet. Bei einem Profilmanager handelt es sich um eine Objektgruppe, die Daten in Form von Anwendungsprofilen enthält. Profilmanager enthalten darüber hinaus eine Subskribentengruppe. Hierbei handelt es sich um eine Liste mit Zieladressen, die dem Profilmanager als Subskribenten zugeordnet sind. Die Profile eines Profilmanagers sind die an die Subskribenten zu verteilenden Konfigurationsdaten. Subskribenten sind verwaltete Einheiten und stehen für die Zielsysteme oder -anwendungen.

Ein Profil ist ein Datencontainer, der von Tivoli-Anwendungen erstellt wird. Die Daten eines Profils werden von der Anwendung festgelegt. CCMS stellt die Satzstruktur und die Datenbank, in der die Daten gespeichert werden, zur Verfügung. Die Daten, die in den

Profilen gespeichert sind, sind das *Modell* für die vom Benutzer gewünschte Darstellung der Daten in der Implementierung auf dem Zielendpunkt. Benutzer können das Modell beliebig aktualisieren, ohne dass die Implementierung davon beeinflusst wird. Die *Ziel*-Konfiguration wird nur dann aktualisiert, wenn ein Verteilungsvorgang ausgeführt wird und eine Verbindung zur Endpunktmethode der Anwendung hergestellt wird. Ist dies der Fall, konvertiert die Endpunktmethode der Anwendung einen Datenstrom mit dem Datenmodell in ein plattformspezifisches Exemplar des Modells. Die Zielimplementierung besteht aus der verwalteten Ressource selbst sowie den Tivoli SecureWay User Administration-spezifischen Codes oder Methoden, die auf der verwalteten Ressource ausgeführt werden.

Beispiel: In Tivoli SecureWay User Administration werden Benutzerdatensätze in Benutzerprofilen gespeichert. Bei einer Verteilung an einen UNIX-Endpunkt werden die Datei **/etc/passwd** und die Referenzkennwortdatei aktualisiert. Bei einer Verteilung an einen Windows NT-Endpunkt wird die NT-SAM-Datenbank aktualisiert. Eine Kopie der in CCMS gespeicherten Daten löst je nach Endpunktart unterschiedliche Aktionen aus. Dieses Verhalten wird im Allgemeinen als *plattformunabhängig* bezeichnet.

Tivoli-Profile

Tivoli SecureWay User Administration ist eine auf Profilen basierende Anwendung. Dies bedeutet, dass verwaltete Definitionseinheiten wie beispielsweise Benutzerkonten und UNIX-Gruppen als Profildatensätze mit beliebigen Attributen dargestellt werden. Allen Attributen sind Namen, Arten, Werte und Markierungen zugeordnet. Darüber hinaus sind allen Datensätzen Schlüssel, interne Markierungen und unterschiedliche Zeitmarken zugeordnet; diese sind weitgehend verdeckt und werden dem Tivoli-Administrator nicht angezeigt. Datensätze bestehen aus Attributen (Namen-/Werte-Paare). Profildatenbanken bestehen aus Tivoli SecureWay User Administration-Datensätzen, einem Datensatz zur Gültigkeitsprüfung und einem Richtlinienstandarddatensatz.

Über CCMS wird die Basisstruktur eines CCMS-Datensatzes definiert. Tivoli SecureWay User Administration erweitert diese Definition um anwendungsspezifische Attribute. Es gibt zwei Möglichkei-

ten für die Ausführung dieses Vorgangs. Die erste Möglichkeit ist die Ausführung als Teil der kompilierten Definition eines Benutzerprofils. Die zweite Möglichkeit ist die Verwendung von AEF. Sie können einem Benutzerprofil Attribute dynamisch hinzufügen, indem Sie den Befehl **waddusrprop** bzw. **waddprop** verwenden. Weitere Informationen finden Sie unter „Der Standardwertegruppendatensatz und die Befehle waddprop, waddusrprop, wgenusrdef" auf Seite 378. Mit Hilfe der auf AEF basierenden Attribute können Endbenutzer die Anwendung erweitern und dieser Benutzer-, Standort- und kundenspezifische Informationen hinzufügen.

Die CCMS-Datenbank kann sich auf herkömmlichen Profilmanagern, Datenbank-Profilmanagern, *datenlosen* Profilmanagern und Profilendpunkten befinden. Die Begriffe Datenbank und datenlos beziehen sich auf die Subskribenten des Profilmanagers und nicht auf den Profilmanager selbst. Beide Profilmanagerarten enthalten Daten. Die Subskribenten, die datenlosen Profilmanagern zugeordnet sind, enthalten jedoch keine Kopien der Profildaten. Die Subskribenten eines Datenbank-Profilmanagers enthalten Kopien der Profildatensätze. Der datenlose Profilmanager wurde zur Implementierung der dreistufigen Architektur eingeführt. Die CCMS-Datenbank wird als Attributgruppe auf Profilmanagern, datenlosen Profilmanagern oder Profilendpunktobjekten implementiert. Die CCMS-Datenbank ist keine relationale Datenbank außerhalb der Tivoli-Objektdatenbank.

Profilmanager-Subskribenten

Profilmanagern können keine oder mehrere Subskribenten zugeordnet sein. Diese Beziehung ist in CCMS elementar; Subskribenten werden entsprechend dem Inhalt vonMitgliedsprofilen im Profilmanager konfiguriert, wenn diese Profile verteilt werden. Profilendpunkte, andere herkömmliche Profilmanager und datenlose Profilmanager können herkömmlichen Profilmanagern als Subskribenten zugeordnet werden. *Profilendpunkte* oder TMA-Endpunkte können datenlosen Profilmanagern als Subskribenten zugeordnet werden.

Bei einem Profilendpunkt handelt es sich um eine Sonderart des Profilmanagers. Ihnen ist genau ein impliziter Subskribent zugeordnet: der verwaltete Knoten, auf dem sich der Profilendpunkt befindet. Verwaltete Knoten implementieren die Profilendpunkt-Schnittstelle.

Verwaltete Knoten dienen also sich selbst als Profilendpunkte. Außer den verwalteten Knoten werden auch noch andere Profilendpunktarten in der Tivoli SecureWay User Administration-Umgebung verwendet. Andere Profilendpunktarten sind: Tivoli SecureWay User Administration-NIS-Domänenobjekte, Tivoli SecureWay User Administration- LDAP-Verbindungen, Tivoli SecureWay User Administration-GSO-Verbindungen und Tivoli SecureWay User Administration-Policy Director-Verbindungen.

So wie Profilmanager und datenlose Profilmanager können Profilendpunkte CCMS-Datensätze enthalten. Profile können von Profilendpunkten an die Anwendungen auf diesem Endpunkt verteilt werden. Beispiel: Benutzerprofile, die an einen verwalteten Knoten verteilt wurden, können auf dem verwalteten Knoten editiert und dann verteilt werden, um die Systemkonfigurationsdateien zu aktualisieren. Der Begriff *datenlos* bezieht sich auf die Subskribenten des Profilmanagers. Die Subskribenten der datenlosen Profilmanager enthalten keine Kopien der Profildatensätze.

Auf TMA-Endpunkten befinden sich keine Objektdatenbanken; sie gelten als datenlos.

Wenn Profilendpunkte datenlosen Profilmanagern als Subskribenten zugeordnet werden, wirkt sich dies auf die Verteilung von Datensätzen aus. Wenn ein Profilendpunkt einem datenlosen Profilmanger als Subskribent zugeordnet wurde und ein Profil vom datenlosen Profilmanager an den Profilendpunkt verteilt wird, wird die CCMS-Datenbank auf dem Profilendpunkt umgangen. Beispiel: Bei der Verteilung eines neuen Benutzerprofils von einem datenlosen Profilmanager an einen verwalteten Knoten werden die Profildatensätze direkt an den Tivoli SecureWay User Administration-Code weitergegeben. Es wird keine Kopie des Benutzerprofils auf dem verwalteten Knoten abgelegt. Dies hat Auswirkungen, wenn Datensätze mit der Profilkopie auf dem verwalteten Knoten zusammengefügt, Datensätze für Verteilungen von exakten Kopien zusammengefügt und UNIX-Systemdateien mit RCS gesichert werden. Weitere Informationen zur Verteilung finden Sie unter „Sonderverarbeitung für Kennwörter bei der Verteilung” auf Seite 365.

Subskribenten auf Datensatzebene

Diese Funktion wird durch Tivoli SecureWay User Administration und nicht durch CCMS implementiert. Wenn feststeht, für welche Datensätze eines Profils CCMS Push-Operationen ausführt, werden alle diese Benutzerdatensätze an alle zugeordnet sein. Auf allen Endpunkten wird die Liste der Subskribenten auf Datensatzebene für alle Benutzerdatensätze durch den Tivoli SecureWay User Administration-Code überprüft, um festzustellen, ob der jeweilige Datensatz an den entsprechenden Endpunkt verteilt werden soll. Wenn der Endpunkt nicht in der RLS-Liste enthalten ist, wird der Datensatz ignoriert. Wenn ein bestimmter Endpunkt kein Subskribent auf Datensatzebene ist, werden dennoch alle AEF-Aktionen ausgeführt, da AEF-Aktionen durch CCMS implementiert werden.

Profilverteilung

Im Folgenden wird aufgezeigt, welche Operationen bei der Verteilung eines Profils ausgeführt werden. Die Verarbeitung dieses Prozesses wird gemeinsam von CCMS und Tivoli SecureWay User Administration ausgeführt.

Die Verarbeitung von Profilen der höchsten Ebene durch Tivoli SecureWay User Administration

- CCMS führt ‘Vorher’-Aktionen auf dem TMR-Server aus.
- Tivoli SecureWay User Administration führt ‘Vorher’-Aktionen für fern angehängte Basisverzeichnisse aus.
- CCMS führt Push-Operationen für Profile aus, was wiederum zur sofortigen Verarbeitung von Profilkopien führt, die unten beschrieben wird.
- Tivoli SecureWay User Administration führt ‘Nachher’-Aktionen für fern angehängte Basisverzeichnisse aus.
- CCMS führt ‘Nachher’-Aktionen auf dem TMR-Server aus.

Sofortige Profilkopieverarbeitung durch CCMS

- CCMS fügt die Informationen eines Profils der höchsten Ebene mit denen eines vorhandenen Profils, das sich auf einer niedrigeren Ebene befindet, zusammen. Dieses Profil ist eine Kopie eines Profils, das einem Subskribentenprofilmanager zugeordnet ist.
- CCMS sendet die zusammengefügten Informationen im Push-Modus an die Profilkopie der nächsten Ebene.

Profilkopieverarbeitung am Zielort

- CCMS fügt auch hier die Informationen des Profils der höheren Ebene mit denen der bereits vorhandenen endgültigen Kopie des Profils zusammen.
- Wenn es sich hierbei um die Verteilung einer exakten Kopie handelt, entspricht diese Endstufe dem CCMS-Punkt für die Zusammenfügung. Die Benutzerdatensätze aller Profile, die über diesen Profilendpunkt bzw. datenlosen Profilmanager verteilt wurden, werden zu einer Liste mit Benutzerdatensätzen zusammengefügt, die von um_update verarbeitet wird.
- **um_update** führt für jeden Benutzerdatensatz folgende Operationen aus:
  - Alle Subskribenten auf Datensatzebene werden überprüft. Wenn der Endpunkt nicht in der Liste enthalten ist, wird der Datensatz übersprungen.
  - Führt ‘Vorher’-Aktionen für das lokale Basisverzeichnis aus.
  - Benutzerkonten werden hinzugefügt/geändert/gelöscht
  - Führt ‘Nachher’-Aktionen für das lokale Basisverzeichnis aus.
- CCMS führt ‘Nachher’-Aktionen auf dem Endpunkt aus.
- Steuerung wird an die TMR-Serververarbeitung zurückgegeben

CCMS und AEF (Application Extension Facility)

CCMS unterstützt AEF-Erweiterungen für auf Profilen basierende Anwendungen, wodurch Profilen benutzerdefinierte Attribute hinzugefügt werden können. Darüber hinaus ermöglicht AEF die Ausführung von Aktionen als Reaktion auf Ereignisse wie 'Erstellen', 'Ändern' und 'Löschen'. Benutzer, die die Daten, die von einem Profil verwaltet werden, erweitern möchten, können Profilen Attribute hinzufügen. Benutzer von Tivoli SecureWay User Administration müssen Benutzerprofilen zur Steuerung der Verwaltung von Benutzerinformationen oftmals Attribute hinzufügen. Beispiel: Administratoren möchten zusätzlich zum Kennwort und Basisverzeichnis Informationen zum Bürostandort des Benutzers und zur Mitarbeiter-ID protokollieren. Mit Hilfe von AEF können dem Benutzerprofil diese Attribute hinzugefügt werden.

Aktionen ordnen der Ausführung eines Skripts eine Änderung im Profil zu (Hinzufügen bzw. Löschen von Benutzern oder Änderung von Attributen). Die Operationen **Hinzufügen** und **Löschen** lösen ein Ereignis für jeden einzelnen Datensatz aus. Die Aktion **Ändern** löst ein Ereignis für jedes einzelne Attribut aus. Aktionen geben Bourne-Shell-Skripts, Korn-Shell-Skripts bzw. Perl-Skripts an, die während einer Profilverteilung ausgeführt werden. CCMS verwaltet für jedes Profil einen Aktionsdatensatz in der Datenbank. Der Aktionsdatensatz enthält Einträge für alle registrierten Aktionen. Sie können auch die Aktion angeben, die auf dem TMR-Server bzw. dem Endpunkt ausgeführt werden soll. Jedem Profilobjekt ist ein Attribut, das so genannte Attribut für anstehende Aktionen zugeordnet, das die Liste mit den für das jeweilige Profil anstehenden Aktionen verwaltet. Da es sich bei Aktionen um Skripts handelt, können diese nur auf Endpunkten ausgeführt werden, die Bourne-Shell, Korn-Shell bzw. Perl unterstützen. Weitere Informationen zur Konfiguration von AEF-Aktionen für Profile finden Sie in der Beschreibung der Befehle **waddaction**, **wlsaction**, **wgetaction** und **wrmaction** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

CCMS-Verteilungsverarbeitung und AEF-Aktionen

Die Verarbeitung von Aktionen auf dem TMR-Server wird einzig und allein durch die Verwendung des Attributs für anstehende Aktionen gesteuert. Wenn die Aktion nicht in der Liste der anstehenden Aktionen aufgeführt ist (über das Attribut), wird sie auf dem TMR-Server nicht ausgeführt. Andererseits sind Endpunktaktionen völlig dynamisch. Welche Aktionen ausgeführt werden, wird durch die Zeitmarken der Datensätze und Attribute und nicht durch die Liste der anstehenden Aktionen festgelegt. Der einzige Vorteil bei der Verwendung des Attributs für anstehende Aktionen ist, dass die Aktionen auf dem TMR-Server schneller ausgeführt werden. Aktionen für verwaltete Knoten werden als Methodenaufrufe implementiert. Wenn ein Aktionsskript auf einem Endpunkt ausgeführt werden muss, wird die Methode **execute_script()** durch CCMS aufgerufen. Dies ist eine in CCMS integrierte Methode zur Ausführung von Bourne-Shell-, Korn-Shell- bzw. Perl-Skripts.

Aktionen für TMA-Endpunkte werden über eine Methode in der Task-Bibliothek implementiert. Zur Verbesserung der Skalierbarkeit werden TMA-Aktionen mit **MDIST** auf die gleiche Weise wie Profildaten an die Endpunkte gesendet. Zur Ausführung von Aktionen auf den Zielendpunkten werden zwei separate **MDIST**-Jobs verwendet. Der erste Job wird vor der Zustellung von Profildaten gestartet, um 'Vorher'-Aktionen auszuführen. Der zweite Job wird nach der Zustellung der Daten gestartet, um 'Nachher'-Aktionen auszuführen.

Eine AEF-Änderungsaktion bezieht sich auf ein einzelnes Attribut und muss denselben Namen wie das Attribut haben. Wenn eine AEF-Änderungsaktion ausgeführt wird, können Sie jedoch nicht davon ausgehen, dass das entsprechende Attribut geändert wurde. CCMS verwaltet nur eine einzige "geändert"-Markierung auf Datensatzebene. Welche Attribute geändert wurden, wird nicht protokolliert. Folglich werden grundsätzlich bei Verteilungen von geänderten Datensätzen *alle* AEF-Aktionen des Typs "geändert" ausgeführt. Dabei ist es unerheblich, ob das Attribut, das einer AEF-Aktion zugeordnet ist, tatsächlich geändert wurde.

Sonderverarbeitung für Kennwörter bei der Verteilung

Der Oneshot-Mechanismus in Tivoli SecureWay User Administration ermöglicht eine Sonderverarbeitung von bestimmten Benutzerattributen während der Verteilung von Benutzerprofildatensätzen an Subskribenten. Es wird davon ausgegangen, dass das Benutzerprofil die meisten Kontendaten exakt widerspiegelt. Wenn eine Push-Operation für einen Datensatz ausgeführt wird, werden diese Daten auf dem Endpunkt überschrieben. Einige lokale Kontendaten können jedoch lokal aktualisiert werden, so dass sich die lokalen Daten erwartungsgemäß von den Serverdaten unterscheiden. Typische Beispiele hierfür sind Kennwörter und Markierungen für den vorzeitigen Ablauf. Benutzer müssen nämlich ihre Kennwörter lokal ändern, um sich an Konten anmelden zu können, deren Kennwörter vorzeitig ablaufen. Da das Kontenattribut des Endpunkts in diesem Fall möglicherweise aktueller als die Benutzerprofildaten ist, müssen die lokalen Daten während der Verteilung beibehalten werden. Diese Attribute werden Oneshot-Attribute genannt, da Sie die Daten auf einem Endpunkt nur ein einziges Mal ändern sollten, und zwar während der ersten Push-Operation nach deren Änderung im Benutzerprofil.

Die aktuelle Implementierung der Oneshot-Attribute geht davon aus, dass nur eine Push-Operation für die Verteilung des geänderten Datensatzes an alle Profilsubskribenten erforderlich ist. Nach Ausführung dieser einen Push-Operation wird das Hot Flag entfernt, so dass das Oneshot-Attribut künftig ignoriert wird. Alle Subskribenten, die während der Push-Operation offline waren, ignorieren bei der erneuten Verteilung des Profils die Änderung am Oneshot-Attribut, obwohl der Datensatz neu für sie ist.

In Tivoli SecureWay User Administration Version 3.7 für UNIX-TMA-Endpunkte, NT-verwaltete Knoten, Windows 2000- und Windows NT-TMA-Endpunkte wurde noch eine weitere Methode zur Änderungssteuerung implementiert, und zwar auf Basis der einzelnen Subskribenten. Bei jeder Verteilung wird allen Oneshot-Attributen eine Versionsnummer zugeteilt. Die Endpunkte protokollieren für jeden einzelnen Profileintrag und jedes einzelne Attribut die Versionen aller empfangenden Oneshot-Attribute. Diese Daten werden in einer kleinen, geschützten Datei auf dem Endpunkt (in der Versionsdatenbank) gespeichert. Auf Grund dieser Implementierung können entsprechende Maßnahmen getroffen werden, wenn ein Endpunkt während einer Verteilung ein Oneshot-Attribut empfängt, das bereits bekannt ist. Wenn die verteilten Oneshot-Daten neu sind, überschreibt der Endpunkt seine lokalen Daten und aktualisiert das Protokoll, in dem die Attributversionen gespeichert sind. Diese Methode ist auch für Teilverteilungen anwendbar. Wenn ein Datensatz an den Subskribenten gesendet wird, stehen genügend Informationen zur Verfügung, um die Daten korrekt zusammenzufügen.

Steuerung der Änderung von Oneshot-Attributen auf Basis des Endpunkt-Status

Für alle Oneshot-Attribute in allen Benutzerprofildatensätzen, die an einen Tivoli SecureWay User Administration-Endpunkt (entweder an einen verteilten Knoten oder Endpunkt) verteilt werden, durchsucht der Endpunkt die Versionsdatenbank nach der CCMS-Datensatzschlüssel/Attributnamen-Kombination. Ob der Endpunkt diese Änderung zulässt, hängt von den Suchergebnissen ab.

Wenn die Versionssuche erfolgreich ist, wird die Versionsnummer des zuletzt verteilten Attributs für diesen Datensatz angezeigt. Wenn sich diese Versionsnummer von der Versionsnummer des empfangenen Attributs unterscheidet, aktualisiert der Endpunkt den Attributwert und speichert die neue Versionsnummer in der Versionsdatenbank. Wenn jedoch die Versionsnummer des zuletzt verteilten Attributs mit der des empfangenen Attributs übereinstimmt, wird die Änderung ignoriert.

Wenn die Versionssuche aus irgendeinem Grund fehlschlägt, greift der Endpunkt auf die klassischen Oneshot-Verhaltensweisen zurück: Ob der Endpunkt die Änderung akzeptiert oder ignoriert, hängt davon ab, ob den Oneshot-Attributen im empfangenen Datensatz ein Hot Flag zugeordnet ist. Wenn dem Attribut ein Hot Flag zugeordnet ist, wird die Änderung akzeptiert und die neue Versionsnummer des Attributs in der Versionsdatenbank gespeichert. Die Versionsdatenbank befindet sich im Verzeichnis $LCF_DATDIR/Tivoli_UA_VersionDB.

Anmerkung: Die Verhaltensweisen von Hot Flags und Attributversionsnummern gelten für Benutzerprofile, die wie folgt verteilt wurden:

- Mit dem Befehl **wdistrib -m -l maintain** (über folgende Option der grafischen Benutzerschnittstelle: **Änderungen in der Profilkopie des Subskribenten erhalten**)
- **wdistrib -m -l over_opts**
- **wdistrib -m -l over_all_no_merge**

Diese Verhaltensweisen gelten nicht für Benutzerprofile, die mit dem Befehl **wdistrib -m -l over_all** verteilt wurden.

In den ersten zwei Spalten der unten angezeigten Tabelle finden Sie eine Zusammenfassung der Verhaltensweisen von Endpunkten, wenn Oneshot-Attribute geändert und Push-Operationen ausgeführt werden.

Versionssuche erfolgreich	Die zuletzt verteilte Version stimmt mit der empfangenen Version überein	Wert des Hot Flags	Endpunkt akzeptiert Änderung	Endpunkt speichert eingehende Version in Datenbank
Ja	Ja	Nicht zutreffend	Nein	Nein
Ja	Nein	Nicht zutreffend	Ja	Ja
Nein	Nicht zutreffend	WAHR	Ja	Ja
Nein	Nicht zutreffend	FALSCH	Nein	Ja

Anmerkung: Wenn wie im letzten Fall die Suche fehlschlägt (meistens weil ein Administrator eine zu große Versionsdatenbank gelöscht hat) und das Hot Flag auf 'Falsch' (FALSE) gesetzt ist, erstellt der Endpunkt eine neue Versionsdatenbank und speichert die Versionsnummer des empfangenen Attributs für künftige Suchvorgänge, obwohl er die zugeordnete Änderung ignoriert.

Oneshot-Attribute anzeigen

Beim Anzeigen eines Oneshot-Attributs in einem Benutzerdatensatz kann nicht ermittelt werden, ob sich dieses Attribut bei der nächsten Verteilung des Benutzerdatensatzes auf die Endpunkte auswirken wird. Dies gilt im Allgemeinen für alle Oneshot-Attribute, ist aber besonders bei Attributen für Kennwörter bei Erstanmeldung von Relevanz.

Beispiel:

```
# wgetusr -E @UserProfile:pm1.up2 user2
Informationen zu Benutzer 'user2':
UNIX-Kennwort bei Erstanmeldung: Disabled
```

In diesem Beispiel erhalten Sie zwar den Status des UNIX-Kennworts bei Erstanmeldung, es geht jedoch nicht hervor, ob bei der nächsten Verteilung von @UserProfile:pm1.up2 der vorzeitige Ablauf von Kennwörtern bei UNIX-Verteilungszielen inaktiviert wird. Auch die GUI-Schaltfläche für die Darstellung und Änderung des UNIX-Kennworts bei Erstanmeldung ist nicht eindeutig. Grund hierfür ist, dass der Wert für das betreffende Attribut keine Aktion ist. DISABLED bedeutet daher nicht, dass der vorzeitige Ablauf inaktiviert wird. Vielmehr wird lediglich der aktuelle Status beschrieben.

Damit Sie wissen, welche Aktion bei der nächsten Verteilung von @UserProfile:pm1.up2 ausgeführt wird, müssen Sie wissen, ob der Wert des Attributs für den vorzeitigen Ablauf seit der letzten Verteilung geändert wurde.

Bei Kennwortänderungen wird empfohlen, eine Verteilung unmittelbar nach der Änderung des Kennworts auszuführen bzw. einzuplanen. Hiermit wird ein fester Zeitpunkt bestimmt, zu dem:

- der neue Kennwortattributwert auf den Endpunkten in Kraft tritt.
- das Kennwortattribut im Benutzerdatensatz nicht aktiv ist und keine Auswirkungen auf nachfolgende Verteilungen hat.

Diese Vorgehensweise sollte in Zusammenhang mit allen Oneshot-Attributen befolgt werden. Wird ein Oneshot-Attribut für einen Benutzer geändert, sollten Sie eine Verteilung dieses Benutzerprofildatensatzes ausführen bzw. planen.

Mit dem folgenden Befehlen können Sie ermitteln, welche Oneshot-Attribute in einem Profil vorhanden sind:

```
wlsusrprop -c @UserProfile:up1
```

Der Einfluss von Verteilungsoptionen auf Benutzerkonten und Kennwörter

Durch die Verteilung eines Profils werden die Systemkonfigurationsdateien der Subskribenten und die Datenbanken mit den Profildaten aktualisiert. Entsprechend den Geschäftsanforderungen gibt es verschiedene Verteilungsoptionen. In den folgenden Abschnitten finden Sie eine Beschreibung der Implementierung mehrstufiger Verteilungen mit Hilfe des Befehls **wdistrib -m** bzw. der GUI-Option zum Verteilen an alle **Subskribentenebenen**. (Weitere Informationen zur Verteilung nur an die nächste Subskribentenebene finden Sie in der Beschreibung des Befehls **wdistrib** im Handbuch *Tivoli SecureWay User Administration Reference Manual*.)

Für alle Profilverteilungsarten gilt:

- Der gesamte Benutzerdatensatz wird an die Zieladresse übertragen. Es ist beispielsweise nicht möglich, ausschließlich UNIX-Daten an UNIX-Zieladressen zu senden.
- Nach der erfolgreichen Verteilung an die entsprechenden Zieladressen werden die Hot Flags in den Profildatensätzen gelöscht. Bei der erneuten Verteilung desselben Profils an eine andere Zieladresse werden Kennwörter zum Beispiel nicht aktualisiert.
- Bei einer erfolgreichen Verteilung an eine beliebige Zieladresse wird die Zeitmarke des Profils, die anzeigt, wann die letzte Push-Operation für das Profil ausgeführt wurde, aktualisiert. Die Profilzeitmarke für die zuletzt ausgeführte Push-Operation wird auf Profilbasis und nicht auf Subskribentenbasis gespeichert. Dies ist für die Bestimmung der Datensätze, die mit der Option ’maintain’ übertragen werden, wichtig.
- Bei allen Änderungen an einem Benutzerdatensatz in einem Benutzerprofil wird die Zeitmarke für die Datensatzänderung aktualisiert (Ausnahme: Wenn Sie einen Datensatz mit dem Befehl **wpasswd -L** ändern, erfolgt keine Aktualisierung, da mit diesem Befehl Endpunktkennwörter ohne Profilverteilung sofort geändert werden können). Dies ist für die Bestimmung der Datensätze, die mit der Option ’maintain’ übertragen werden, wichtig.

- Während einer Verteilung ist das Profil gesperrt und kann nicht aktualisiert werden.
- Der Versuch wird unternommen, alle AEF-Aktionen, für die die Ausführung auf dem Client angegeben wurde, auf allen Zieladressen einer Verteilung auszuführen. Erstellen Sie durchdachte Skripts für AEF-Aktionen, und testen Sie diese sorgfältig.
- Sie können das Protokoll der Subskribentenverteilungen eines Profilmanagers prüfen, indem Sie folgenden Befehl ausgeben:

  ```
  wgetsub -l @ProfileManager:Profilmanagername
  ```

wdistrib -m -l maintain

Für eine Profilverteilung mit der Option 'maintain' (die entsprechende Option auf der grafischen Benutzerschnittstelle ist **Änderungen in der Profilkopie des Subskribenten erhalten**) gilt:

- Änderungen in untergeordneten Kopien des Profils werden beibehalten. Alle lokalen Änderungen an den Systemkonten auf dem Endpunkt werden jedoch durch diese Verteilung überschrieben.
- Alle Systemattribute für Benutzer werden mit den Profildaten aktualisiert.

  Anmerkung: Folgende Ausnahme gilt: Besondere Attribute für Profile (wie beispielsweise Kennwörter) werden nur aktualisiert, wenn Sie im Profil explizit geändert wurden und die zugehörige Attributversionsnummer inkrementiert bzw. das Hot Flag gesetzt wurde.
- Es werden nur die Datensätze, die seit der letzten Verteilung geändert wurden, verteilt (die Zeitmarken für Datensatzänderungen werden mit den Zeitmarken für die letzte Push-Operation für das Profil verglichen).

- Wenn der Zugriff auf Subskribenten nicht möglich ist, werden bei der nächsten Verteilung desselben Typs nicht dieselben Profilaktualisierungen an diese Subskribenten verteilt, da die Datensatzänderung nicht aktueller als die letzte Push-Operation für das Profil ist und vorhandene Hot Flags entfernt wurden.
- Diese Art der Profilverteilung wird am häufigsten angewendet, da nur die geänderten Datensätze weitergegeben werden und Endbenutzer ihre eigenen Kennwörter mit den betriebssystemeigenen Tools verwalten können. Beispiel: Die meisten UNIX-Benutzer verwenden üblicherweise /bin/passwd zur Kennwortänderung. Die meisten NT-Benutzer verwenden die Option 'Kennwort ändern' in der Anzeige 'Windows NT-Sicherheit' (ctl/alt/del).

wdistrib -m -l over_opts (keine äquivalente Option auf der grafischen Benutzerschnittstelle (GUI))

Dies entspricht dem Befehl **wdistrib -m -l maintain** mit der Ausnahme, dass alle Datensätze im Profil verteilt werden. Dennoch können Endbenutzer ihre eigenen Kennwörter mit den betriebssystemeigenen Tools ändern. Dieser Profilverteilungsmodus wird häufig gewählt, wenn ein neuer Subskribent hinzugefügt wird oder wenn der Zugriff auf einen vorhandenen Subskribenten nicht möglich ist und der Tivoli-Administrator diesen Subskribenten aktualisieren möchte.

wdistrib -m -l over_all

Für eine Profilverteilung unter Verwendung der Option **over_all**. Dieser Profilverteilungsmodus wird in Geschäftsumgebungen angewendet, für die ein hohes Maß an Sicherheit erforderlich ist. Über diesen Verteilungsmodus werden alle Konten gelöscht, die lokal hinzugefügt wurden. Darüber hinaus müssen die Endbenutzer ihre Kennwörter unter Verwendung von Tivoli SecureWay User Administration verwalten. Stellen Sie vor Verwendung dieses Verteilungsmodus in einer Arbeitsumgebung sicher, dass Sie sich der Auswirkungen bewusst sind. (Wählen Sie auf der grafischen Benutzerschnittstelle (GUI) die Option **Profil der Subskribenten EXAKT mit diesem Profil abgleichen** aus):

- Verteilt alle Datensätze im Profil
- Die Daten des im Push-Modus gesendeten Profils überschreiben Änderungen in den untergeordneten Kopien dieses Profils und in den Systemdateien.
- Alle Kennwörter auf Verteilungszielen werden durch die Werte im Profil ersetzt.
- Auf UNIX-Systemen verschlüsselt Tivoli SecureWay User Administration das Kennwort aus dem Profil mit dem Verschlüsselungsbasiswert aus dem UNIX-Systemkennwort, um festzustellen, ob diese identisch sind. Wenn das Systemkennwort dem Kennwort im Profil entspricht, wird das Systemkennwort nicht ersetzt. Dadurch wird verhindert, dass das Datum der letzten Kennwortänderung im System fälschlicherweise aktualisiert wird. Darüber hinaus wird sicher gestellt, dass die Prioritätssteuerung nach Verweildauer für UNIX-Kennwörter ordnungsgemäß funktioniert.
- Die Benutzerdatensätze in allen Profilen, die zuvor an eine Zieladresse verteilt wurden, werden zusammengefügt und auf dem System aktualisiert. Andere Konten auf dem Verteilungszielobjekt werden gelöscht! Ausnahme: geschützte Konten wie das Root-Konto unter UNIX und das Administratorkonto unter NT. Weitere Informationen zu geschützten Konten finden Sie im Handbuch *Tivoli SecureWay User Administration Reference Manual*.
  - Wenn die Verteilungsziele verwaltete Knoten sind, die herkömmlichen Profilmanagern als Subskribenten zugeordnet sind, werden die Daten auf dem Endpunkt zusammengefügt.
  - Wenn die Verteilungsziele verwaltete Knoten oder TMA-Endpunkte sind, die einem datenlosen Profilmanager als Subskribenten zugeordnet sind, werden die Daten im datenlosen Profilmanager zusammengefügt. Aus diesem Grund ist es wichtig, dass die TMA-Endpunkte, wenn diese Zieladressen für Verteilungen sind, einem einzelnen datenlosen Profilmanager als Subskribenten zugeordnet werden, damit die Profile ordnungsgemäß zusammengefügt werden.

- Nicht für alle Betriebssystemtypen verfügbar (NW, OS/390)

wdistrib -m -l over_all_no_merge (keine äquivalente Option auf der grafischen Benutzerschnittstelle (GUI))

Dieser Befehl entspricht dem Befehl **wdistrib -m -l over_all** mit der Ausnahme, dass nur die Kennwörter auf den Verteilungszielen durch das Profil aktualisiert werden, denen ein Hot Flag bzw. eine Attributsversionsnummer zugeordnet ist, die anzeigen, dass es sich um ein aktives Kennwort handelt. Mit diesem Profilverteilungsmodus können Sie die Konsistenz der Systemdaten mit Profildaten sicherstellen und dennoch den Endbenutzern die Steuerung ihrer eigenen Kennwörter unter Verwendung von betriebssystemeigenen Tools ermöglichen.

Benutzer- und Gruppen-Indexdatenbanken und der Befehl wchkadmdb

Tivoli SecureWay User Administration verwaltet drei Arten von Hilfsdatenbanken in der TNR (TNR = Tivoli Name Registry), die als Referenz für die Profildatensätze, die in CCMS gespeichert sind, dienen.

- Die Benutzernamensdatenbank, die Benutzer anhand ihres Anmeldenamens suchen
- Die Benutzer-ID-Datenbank, die Benutzer anhand ihrer UNIX-Benutzer-ID suchen
- Die Datenbank der Benutzersuchfunktion, die Benutzer anhand ihres tatsächlichen Namens suchen

Über diese Datenbanken kann durch eine Eingabe der entsprechende CCMS-Satzschlüssel zum Abrufen des Benutzerdatensatzes festgestellt werden.

Mit dem Befehl **wchkadmdb** können Fehler diagnostiziert und behoben werden. Er wird vor allem dann von der Tivoli-Kundenunterstützung zur Fehlerbehebung verwendet, wenn die Profildaten von den Indexdatenbanken nicht mehr richtig gespiegelt werden. Der

Befehl ist nicht für regelmäßig durchgeführte Bereinigungen der Arbeitsplatzumgebung gedacht. Wenn der Befehl während der Aktualisierung von Benutzern oder Gruppen durch das System ausgeführt wird, werden möglicherweise fehlerhafte Einträge in die Datenbanken geschrieben. Er kann jedoch ohne Weiteres im Anzeigemodus ausgeführt werden, um Inkonsistenzen festzustellen.

Mit dem Befehl **wchkadmdb** werden Informationen aus Benutzer- und Gruppenprofilen mit den in diesen Hilfsdatenbanken enthaltenen Informationen verglichen, um mögliche Inkonsistenzen festzustellen. Auf Wunsch können diese Inkonsistenzen mit diesem Befehl durch Aktualisierungen der entsprechenden Datenbanken behoben werden. Mit dem Befehl **wchkadmdb** können die Daten in Benutzer- und Gruppenprofilen nicht geändert werden.

Die folgende Tabelle veranschaulicht die Beziehung zwischen dem Benutzerprofil und den drei Datenbankarten:

Das Benutzerprofil

Datensatzschlüssel	tatsächlicher Name	Anmeldename	Benutzer-ID
pOID_1	Tim Jones	tim (UNIX)	100
pOID_2	Bill Best	bill (NT)	-
pOID_3	Nancy Dee	nancy (UNIX, NT)	101
pOID_4	Lars Smitt	lars (UNIX, NT)	102
pOID_5	Lisa Sparks	lisa (UNIX)	100
pOID_6	Dave Hill	dave (NT)	-

Die Benutzernamensdatenbank

Datenbankschlüssel	Beschreibung	Datensatzschlüssel
tim	Anmeldung	pOID_1
bill	nt_Anmeldung	pOID_2
nancy	Anmeldung, nt_Anmeldung	pOID_3
lars	Anmeldung, nt_Anmeldung	pOID_4

Datenbankschlüssel	Beschreibung	Datensatzschlüssel
lisa	Anmeldung	pOID_5
dave	nt_Anmeldung	pOID_6

Anmerkung: In der Praxis würde die Benutzernamensdatenbank auch Einträge für den allgemeinen Anmeldenamen sso_login und möglicherweise NetWare-Anmeldenamen enthalten. Sie kann für denselben Benutzerdatensatz auch verschiedene Anmeldenamen für jede Anmeldung enthalten. Die Gruppennamendatenbank entspricht ungefähr der Benutzernamensdatenbank und enthält UNIX-Gruppennamen, die in Gruppenprofilen verwendet werden.

Die Benutzer-ID-Datenbank

Datenbankschlüssel	Beschreibung	Datensatzschlüssel
100	Benutzer-ID	pOID_1
101	Benutzer-ID	pOID_2
102	Benutzer-ID	pOID_3
103	Benutzer-ID	pOID_4
104	Benutzer-ID	pOID_5
105	Benutzer-ID	pOID_6

Anmerkung: Die Gruppen-ID-Datenbank und die Prüf-ID-Datenbank sind der Benutzer-ID-Datenbank ähnlich. Die Gruppen-ID-Datenbank enthält die UNIX-Gruppen-IDs, die in Gruppenprofilen verwendet werden und die Prüf-ID-Datenbank enthält die in Gruppenprofilen verwendeten UNIX-Prüf-IDs.

Die Datenbank der Benutzersuchfunktion

Datenbankschlüssel	Beschreibung	Datensatzschlüssel
Tim Jones	tatsächlicher Name	pOID_1

Datenbankschlüssel	Beschreibung	Datensatzschlüssel
Bill Best	tatsächlicher Name	pOID_2
Nancy Dee	tatsächlicher Name	pOID_3
Lars Smitt	tatsächlicher Name	pOID_4
Lisa Sparks	tatsächlicher Name	pOID_5
Dave Hill	nt_Anmeldung	pOID_6

Das Symbol der Benutzersuchfunktion auf der Tivoli-Arbeitsoberfläche ermöglicht eine bequeme Benutzerverwaltung. Die Leistung der Benutzersuchfunktion wurde für Tivoli SecureWay User Administration Version 3.7 wesentlich verbessert, indem eine neue Datenbank hinzugefügt wurde, in der die in der Benutzersuchfunktion gespeicherten Daten gespiegelt werden. Die Implementierung dieser neuen Datenbank erfolgt durch die Berkeley-Datenbank der Firma Sleepycat Software. Hierbei handelt es sich um ein schnelles, einfaches und kompaktes Paket, das speziell für eingebettete Anwendungen entwickelt wurde.

Anmerkungen:

1. Die w*loc-Befehle verwenden weiterhin die TNR-Version und aktualisieren dann die Datenbanktabellen.
2. Die Benutzersuchfunktion kann derzeit keine Informationen von anderen verbundenen TMRs anzeigen; es werden nur Informationen für Benutzer in der lokalen TMR angezeigt.
3. Die BerkeleyDB-Komponentendateien befinden sich im Verzeichnis $DBDIR/TUA_BerkeleyDB auf dem TMR-Server.

```
ls -l $DBDIR/TUA_BerkeleyDB
Gesamtsumme 2996
rw-r—r--    1 root     root         Berkeley_DB_errlog
rwxr-xr-x   1 root     root         __db.001
rwxr-xr-x   1 root     root         __db.002
rwxr-xr-x   1 root     root         __db.003
rwxr-xr-x   1 root     root         __db.004
rwxr-xr-x   1 root     root         __db.005
rwxr-xr-x   1 root     root         __account.db
rwxr-xr-x   1 root     root         log.0000000001
rwxr-xr-x   1 root     root         uLoc.idx
rwxr-xr-x   1 root     root         uLoc_r.idx
```

Anmerkung: Wenn diese Dateien zu viel Speicherplatz belegen, können Sie alle Dateien in diesem Verzeichnis löschen und den Befehl **winitulocdb** -l ausführen, um die Berkeley-Datenbank zu initialisieren. Für eine TMR im Ruhemodus sollte der Befehl **winitulocdb -l** verwendet werden. Die Zeit, die für die Ausführung des Befehls **winitulocdb -l** erforderlich ist, entspricht ungefähr der Zeit, die für die Ausführung von **wlslocs @LocatorDatabase:UserLocator** benötigt wird.

Der Standardwertegruppendatensatz und die Befehle waddprop, waddusrprop, wgenusrdef

Alle Profile enthalten einen einzelnen Standardwertegruppendatensatz. Diese Datensätze enthalten einen Eintrag für jedes Attribut, das in einem Benutzerdatensatz vorkommen kann. Die Attributeinträge enthalten:

- die Standardwertegruppe für dieses Attribut
- die unterschiedlichen Markierungen für dieses Attribut (änderungsgesteuert, verschlüsselt, Anmeldung, Kennwort, Anzeige in Tabellenansicht des Profils, versionsgesteuert)

Um einem Benutzerprofil ein AEF-Attribut hinzuzufügen, können Sie die Befehle **waddprop** oder **waddusrprop** verwenden. Zwischen diesen Befehlen gibt es bedeutende Unterschiede:

- Mit dem Befehl **waddprop** wird dem Standardwertegruppendatensatz des Profils und allen Datensätzen im Profil ein benutzerdefiniertes Merkmal hinzugefügt.
- Mit dem Befehl **waddusrprop** wird dem Standardwertegruppendatensatz des Profils ein benutzerdefiniertes Merkmal hinzugefügt. Den vorhandenen Datensätzen im Profil wird dieses Merkmal jedoch nicht hinzugefügt. Erst wenn das Merkmal für einen Datensatz gesetzt wurde, ist es im Datensatz physisch vorhanden. Für alle neuen Datensätze, die dem Profil nach der Ausführung des Befehls waddusrprop hinzugefügt wurden, ist dieses Merkmal physisch vorhanden, wenn die Verwendung der Standardwertegruppe festgelegt wurde.

Der Befehl **waddprop** sollte verwendet werden, wenn eine AEF-Aktion das neue Merkmal als Argument verwendet. Andernfalls sollten Sie den Befehl **waddusrprop** verwenden. Wenn sich in Ihrem Profil bereits viele Benutzerdatensätze befinden, kann das Hinzufügen eines Merkmals mit dem Befehl **waddprop** sehr viel Zeit in Anspruch nehmen.

Ein praktisches Beispiel: Während der Aktualisierung von Tivoli SecureWay User Administration Version 3.6.2 auf Tivoli SecureWay User Administration Version 3.7 werden dem Standardwertegruppendatensatz der vorhandenen Benutzerprofile unter Verwendung des Befehls **waddusrprop** viele neue Attribute für Windows 2000 hinzugefügt. Nach der Beendigung der Aktualisierungen, können Kunden, die Windows 2000-Benutzerkonten verwalten möchten, die Standardwertegruppe und die Richtlinie für Gültigkeitsprüfung ihren Bedürfnissen entsprechend anpassen. Mit dem Befehl **wgenusrdef -e W2K** werden allen Benutzerdatensätzen für die angegebenen Benutzerprofile die entsprechenden Attributwerte hinzugefügt.

Weitere Veröffentlichungen

Das White Paper zu *Tivoli's Configuration and Change Management System* finden Sie unter dem Abschnitt 'Tivoli Field Guides' auf der Website der Tivoli-Unterstützung unter folgender Adresse: http://www.tivoli.com/support.

Das Redbook zu *Enterprise Security Management with Tivoli* (SG24-5520) finden Sie auf der Website für Redbooks unter folgender Adresse: http://www.redbooks.ibm.com.

Das Kapitel über die Konfigurationsverwaltung finden Sie im *Tivoli Management Framework Benutzerhandbuch*.

A

AS/400-Benutzer verwalten

Systemadministratoren müssen unter Umständen viel Zeit für die Verwaltung von Benutzer- und Gruppenkonten in einem großen Unternehmen aufwenden. Benutzerkonten werden entsprechend den Bedürfnissen der Benutzer und des Unternehmens ständig hinzugefügt, entfernt und aktualisiert.

Das Betriebssystem AS/400 (OS/400) stellt zahlreiche Funktionen zur Benutzerverwaltung zur Verfügung und speichert bestimmte Benutzerinformationen in eigens dafür entworfenen Objekten, den so genannten *USRPRF-Objekten.

Vorteile einer Verwaltung von AS/400-Benutzerkonten über Tivoli

Tivoli SecureWay User Administration for AS/400 stellt die Tools zur Verfügung, die Sie zur Verwaltung von Benutzerkonten unter OS/400 benötigen und integriert diese Unterstützung in andere Betriebssysteme im Netzwerk. Dieses Produkt enthält folgende Benutzer- und Gruppenverwaltungsfunktionen:

- Eine einheitliche Grafikschnittstelle für die Verwaltung von AS/400-, UNIX-, Windows NT- und NetWare-Benutzerkonten
- Schablonen, mit denen Sie durch Eingabe weniger Daten einen vollständigen Datensatz erstellen können
- Zentrale Position zum schnellen Lokalisieren eines bestimmten Benutzerdatensatzes

- Einzelanmeldungsunterstützung
- Zentrale Administratorsteuerung von Konten in Kombination mit begrenzter Benutzereingabesteuerung
- Verwaltung von allgemeinen Benutzerinformationen sowie von AS/400- UNIX-, Windows NT- und NetWare-Benutzerinformationen in einem Benutzerdatensatz

Hintergrundinformationen zur Verwendung der AS/400-Unterstützung finden Sie im Handbuch *Tivoli SecureWay User Administration Management Handbuch*:

- Funktionsweise der Benutzer- und Gruppenverwaltung
- Komponenten von Benutzer- und Gruppenkonten
- Benutzer- und Gruppenprofile
- Richtlinien für Benutzer- und Gruppenprofile
- OnePassword
- Kennwortsteuerung
- Benutzersuchfunktion
- Datensätze sperren
- Sicherheitsverwaltung
- Beispiele für die Verwaltung vieler Benutzer

User Administration for AS/400 verwenden

Tivoli SecureWay User Administration for AS/400 ist eine auf Profilen basierende Anwendung, die unter AS/400 für die Verwaltung von AS/400-Benutzerprofilen eingesetzt wird. Mit diesem Produkt können Sie Datensätze auf einem beliebigen Endpunkt an ein Benutzerprofil weitergeben. Wenn Sie die Datensätze des Profils aktualisiert haben, können Sie das Profil anschließend an beliebige AS/400-Endpunkte verteilen.

Darüber hinaus können Sie AS/400-Benutzerprofile auf verschiedenen Systemen zentral verwalten und organisieren, indem Sie das zu

Grunde liegende Gerüst und die Tools, die von Tivoli Management Framework und Tivoli SecureWay User Administration zur Verfügung gestellt werden, verwenden.

Mit AS/400-Attributen und -Endpunkten arbeiten

Die AS/400-Attribute, die mit Tivoli SecureWay User Administration for AS/400 verwaltet werden können, stehen in direktem Zusammenhang zu OS/400-Befehlen, die zum Ändern, Prüfen und Löschen von AS/400-Benutzerprofilen verwendet werden. Die Tivoli-Arbeitsoberfläche ermöglicht die Verwaltung der AS/400-Attribute mit Hilfe der folgenden Unterkategorien der neuen OS/400-Kategorie:

- OS/400-Protokollierung
- OS/400-Verzeichnis
- OS/400-Datensichtgerätsitzung
- OS/400-Gruppenzugehörigkeit
- OS/400-International
- OS/400-Anmeldung
- OS/400-Ausgabe
- OS/400-Kennwort
- OS/400-Berechtigungen
- OS/400-Sitzungsinitialisierung
- Besondere OS/400-Optionen

AS/400-spezifische Funktionen

Die Benutzerverwaltungsfunktionen sind mit Hilfe eines benutzerdefinierten Codes, der die Informationen zwischen dem Tivoli- und dem OS/400-Benutzerprofilformat umsetzt, auf AS/400-Systeme erweitert worden. Die folgenden Funktionen sind verfügbar:

- Erstellen und Ändern von *USRPRF-Objekten und -Attributen
- Löschen von *USRPRF-Objekten
- Basisverwaltung von *USRPRF-Objekten

Weitergeben/Suchen

Sie können über die Tivoli-Arbeitsoberfläche AS/400-Benutzerprofile an AS/400-Endpunkte weitergeben. Es wird empfohlen, die Profile logischen Verwaltungsgruppen zuzuordnen, die auf die Bedürfnisse Ihres Unternehmens zugeschnitten sind. Sie können auch den Befehl **wpopusrs** verwenden, um ausgewählte Benutzerprofile an einen AS/400-Endpunkt weiterzugeben. Weitere Informationen zum Erstellen und Weitergeben von AS/400-Benutzerprofilen finden Sie im Handbuch *Tivoli SecureWay User Administration Management Handbuch*. In diesem Dokument finden Sie außerdem die in der Befehlszeile zu verwendende Syntax und Beispiele für den Befehl **wpopusrs**.

Anmerkung: Profile, deren Namen mit dem Buchstaben “Q” beginnen, können nicht über die grafische Benutzerschnittstelle (GUI) weitergegeben werden. Sie können sie über die Befehlszeilenschnittstelle (CLI) weitergeben.

Verteilen/Aktualisieren

Sie können unter Verwendung der grafischen Benutzerschnittstelle oder des Befehls **wdistrib** modifizierte Datensätze verteilen. Der AS/400-Endpunkt empfängt die Daten und nimmt die Änderungen an den AS/400-Benutzerprofilen vor.

Kennwörter

Tivoli verwaltet AS/400-Benutzerkennwörter wie folgt:

- Durch Ändern des Kennworts auf dem AS/400-System. Wenn ein Kennwort mit OS/400-Befehlen geändert wird, wird das Kennwort erst dann mit dem Kennwort des Tivoli-Benutzerprofils überschrieben, wenn das Kennwort des Tivoli-Benutzerprofils explizit geändert wurde.
- Durch Ändern des Attributs **OS400_PassW** über die Tivoli-Arbeitsoberfläche.
- Durch Ausführen des Befehls **wpasswd** über die Befehlszeilenschnittstelle.

- Durch Ändern des allgemeinen Kennworts mit dem Web-Tool **OnePassword**, über das das OS/400-Kennwort geändert wird. Dies wird auch mit der Option **–L** im Befehl **wpasswd** angegeben.

Wenn ein Benutzerprofil an einen AS/400-Endpunkt weitergegeben wird, ordnet Tivoli SecureWay User Administration dem Attribut **OS400_PassW** den Wert des Attributs **OS400_Login** zu. Sie müssen diese Konventionen beachten, wenn Sie Benutzerprofile an Systeme verteilen, in denen Kennwörter und Anmeldenamen nicht identisch sein dürfen.

Sonderfunktionen für AS/400

Tivoli SecureWay User Administration stellt die folgenden Funktionen für AS/400-Systeme zur Verfügung:

- Das Löschen von AS/400-Benutzerprofilen anpassen. Verwenden Sie die Attribute **OS400_DLT_Action** und **OS400_DTL_NewOwn** zur Angabe der Aktionen, die für Objekte, die zu löschenden AS/400-Benutzerprofilen angehören, ausgeführt werden sollen.
- Gruppenzugehörigkeit auf AS/400-Endpunkten steuern. Verwenden Sie die Attribute **OS400_Prim_GRP** und **OS400_Supp_GRPs**, um die Gruppenzugehörigkeit auf AS/400-Endpunkten zu steuern.
- Ein Skript, das Ihnen hilft, Benutzerprofile in kleineren Einheiten zu verwalten.

Verwenden Sie das Skript **w4getusers.pl**, um Dateien für die Verwendung mit dem Befehl **wpopusrs -f** zu erstellen. Das Skript befindet sich im Verzeichnis **/usr/Tivoli/bin/lcf_bundle/generic**. Im folgenden Beispiel wird die Syntax für den Befehl **w4getusr.pl** und dessen Parameter aufgezeigt:

```
root@ibmtmp1 [161]./w4getusr.pl

  Syntax:./w4getusr.pl <Option> Host-Name
  -d <dir> Zielverzeichnis für Ausgabedateien
  -n <Number> Maximale Anzahl an Einträgen in den Dateien
```

```
root@ibmtmp1 [164]mkdir /tmp/dddd

root@ibmtmp1 [166]./w4getusr.pl -d /tmp/dddd -n 10 rocket

/tmp/dddd

Maschine 'rocket' konnte NICHT in netrc gefunden werden

/tmp/dddd

Es wird ein Benutzerkonto benötigt. Bitte geben Sie einen Namen ein
bzw. drücken Sie die Eingabetaste zur Verwendung eines [Standardwerts]

Anmeldename für rocket ([QSECOFR]): nlloyd
Geben Sie ein neues Kennwort für 'nlloyd' ein:
Zurückgegebene Gesamtmenge : 117250 root@ibmtmp1 [167]ls /tmp/dddd
usr0 usr1  usr2  usr3  usr4  usr5  usr6  usr7
```

Diese Befehlsfolge erstellt im Zielverzeichnis eine geordnete Liste mit Dateien. Sie können diese Dateien mit dem Befehl **wpopusrs** verwenden, um Daten aus den angegebenen Dateien an ein Benutzerprofil weiterzugeben.

AS/400-spezifische Benutzerinformationen

In der folgenden Tabelle werden die AS/400-Attribute und die zugehörigen Werte, die durch die Befehle **CHGUSRPRF**, **CHGUSRAUD** und **DLTUSRPRF** zugeordnet werden, angezeigt. Bei Verwendung der Tivoli-Arbeitsoberfläche werden diese Werte mit den AS/400-Attributen angezeigt. Bei Verwendung der Befehlszeile müssen Sie die AS/400-Attribute mit den zugehörigen Werten eingeben.

Weitere Informationen zum Erstellen neuer Benutzerkonten über die Tivoli-Arbeitsoberfläche oder über die Befehlszeile finden Sie im *Tivoli SecureWay User Administration Management Handbuch*.

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_Accounting_Code Gibt den Berechnungscode an, der diesem Benutzerprofil zugeordnet ist.	***BLANK** *Endpunktname* Ein Endpunktname (bis zu 15 Zeichen)
OS400_Assist_Level Gibt die Ebene des verfügbaren Hilfetextes an.	***SYSVAL** ***BASIC** ***INTERMED** ***ADVANCED**
OS400_Attention_PGM Gibt das Abrufprogramm an, das diesem Benutzer zugeordnet ist.	***NONE** ***SYSVAL** ***ASSIST** *Programm* Ein gültiger Programmname im Format LIB/PROGRAM
OS400_Authority Gibt die Berechtigung an, die Sie Benutzern zuteilen, die über keine bestimmte Berechtigung für das Objekt verfügen, die in keiner Berechtigungsliste aufgeführt sind und deren Gruppenprofil keine bestimmte Berechtigung für das Objekt zugeordnet ist.	***EXCLUDE** ***ALL** ***CHANGE** ***USE**
OS400_CCSID Gibt die CCSID für dieses Profil an. Wird zu landessprachlichen Zwecken verwendet.	***SYSVAL** ***HEX** *ccsid* Eine AS/400-CCSID
OS400_Change_Rollkey Gibt an, ob bei Verwendung der Blättertaste den Systemstandardaktionen entgegengesetzte Aktionen ausgeführt werden.	***YES** ***NO**

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_CharID_Control Gibt die Zeichen-ID-Steuerung (CHRIDCTL) für den Job an. Dieses Attribut steuert die Art der CCSID-Konvertierung für Anzeigedateien, Druckerdateien und Anzeigengruppen. Dieses Attribut wird verwendet, wenn der Sonderwert *CHRIDCTL für den Befehlsparameter CHRID in den Befehlen 'Erstellen', 'Ändern' und 'Überschreiben' für Anzeigedateien, Druckerdateien und Anzeigengruppen angegeben wurde.	***SYSVAL** ***DEVD** ***JOBCCSID**
OS400_Class Gibt an, welcher Klasse das Benutzerprofil angehört.	***USER** ***SYSOPR** ***PGMR** ***SECADM** ***SECOFR**
OS400_Command_Audit Gibt an, ob CL-Befehlsfolgen und -Prozeduren für das Benutzerprofil protokolliert werden.	***YES** ***NO**
OS400_Country Gibt die Landes-ID für dieses Profil an. Wird zu landessprachlichen Zwecken verwendet.	***SYSVAL** *Landes-ID* Eine AS/400-Landes-ID
OS400_Current_Lib Gibt den Namen der Bibliothek an, die dem derzeit ausgeführten Job zugeordnet ist.	***CRTDFT** *Name* Ein gültiger AS/400-Bibliotheksname (10 Zeichen oder weniger)
OS400_Directory Gibt den Pfadnamen für das Basisverzeichnis des Benutzerprofils an.	***USRPRF** *Pfad* Ein durch "/" begrenzter Pfad für das Basisverzeichnis

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_Display_Help Gibt an, ob der Onlinehilfetext als Gesamtanzeige erscheint oder in einem Fenster angezeigt wird.	***YES** ***NO**
OS400_DLT_Action Gibt die Aktion an, die beim Löschen des Benutzerprofils ausgeführt wird. Vor dem Löschen eines Benutzerprofils müssen alle Objekte, die diesem Benutzerprofil zugeordnet sind, gelöscht werden oder an einen anderen Besitzer übertragen werden. **Anmerkung:** Dieses Attribut ist eine Schnittstelle zum Befehl **DLTUSRPRF**.	***NODLT** ***DLT** ***CHGOWN** *Name*
OS400_DLT_Grp_Action Gibt die Art der Operationen an, die für Objekte ausgeführt werden, deren Primärgruppe das zu löschende Benutzerprofil ist. **Anmerkung:** Dieses Attribut ist dem Primärgruppenwert im Parameter **PGPOPT** des Befehls **DLTUSRPRF** zugeordnet.	***NOCHG** ***CHGPGP**
OS400_DLT_Grp_Authority Gibt die neue Berechtigung an, über die die neue Primärgruppe bezüglich des zu übertragenden Objekts verfügen soll. **Anmerkung:** Dieses Attribut ist der neuen Primärgruppenberechtigung des Parameters **PGPOPT** im Befehl **DLTUSRPRF** zugeordnet.	***OLDPGP** ***PRIVATE** ***ALL** ***CHANGE** ***USE** ***EXCLUDE**

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_DLT_Grp_NewOwn Gibt das Benutzerprofil an, dass der neue Primärgruppenbesitzer aller Objekte, denen das zu löschende Benutzerprofil als Primärgruppe zugeordnet ist, sein wird. **Anmerkung:** Dieses Attribut ist der neuen Primärgruppe des Parameters **PGPOPT** im Befehl **DLTUSRPRF** zugeordnet.	***NONE** *Name* Ein gültiger AS/400-Benutzerprofilname.
OS400_DLT_NewOwn Gibt den Besitzer an, an den die Objekte übertragen werden, wenn das Benutzerprofil auf AS/400-Systemen gelöscht wird.	***CHGOWN** *Name*
OS400_Document_Password Gibt das Dokumentkennwort an, mit dessen Hilfe DIA-Benutzer (DIA = Document Interchange Architecture) verhindern können, dass persönliche Verteilungen von unbefugten Mitarbeitern verwendet werden.	*Kennwort*
OS400_Group_Authority Gibt die Berechtigung an, die dem Gruppenprofil für neue Objekte erteilt wurden.	***NONE** ***ALL** ***CHANGE** ***USE** ***EXCLUDE**
OS400_Group_Authority_Type Gibt den Berechtigungstyp an, der dem Gruppenprofil für neu erstellte Objekte erteilt wurde.	***PRIVATE** ***PGP**

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_Group_ID Gibt die Gruppen-ID-Nummer (GID-Nummer) für dieses Benutzerprofil an. Die Gruppen-ID wird zur Identifizierung des Gruppenprofils verwendet, wenn ein Mitglied der Gruppe das Verzeichnisdateisystem verwendet.	***NONE** ***GEN** *Dezimalzahl* 1 bis 4294967294
OS400_Initial_Menu Gibt den Namen des Anfangsmenüs an, das bei Anmeldung dieses Benutzers angezeigt wird.	***SIGNOFF** *Anfangsmenü* Ein gültiger Menüname im Format LIB/MENU
OS400_Initial_PGM Gibt den Namen des Startprogramms an, das bei Anmeldung dieses Benutzers aufgerufen wird.	***NONE** *Startprogramm* Ein Programmname im Format LIB/PROGRAM
OS400_JOBD Gibt den Namen der Jobbeschreibung an, die für Jobs verwendet wird, die über Eingaben an Workstations des Subsystems gestartet werden. Wenn die Jobbeschreibung bei Erstellung des Benutzerprofils nicht vorhanden ist, muss ein Bibliotheksqualifikationsmerkmal angegeben werden (da sich die Jobbeschreibung im Benutzerprofil befindet). **Anmerkung:** Für Schlüsselwortwerte außer für **QDFTJOB** müssen Sie den Pfad für diesen Namen angeben.	***QDFTJOB** ***LIBL** ***CURLIB** *Bibliotheksname* Der Name der Bibliothek, in der sich die Jobbeschreibung befindet
OS400_Job_Audit Gibt an, ob alle Informationen zum Starten und Stoppen des Jobs für diesen Benutzer geprüft werden.	***YES** ***NO**

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_KBD_Buffering Gibt die Art des zu verwendenden Tastaturpuffers, falls vorhanden, an oder ermöglicht die Übernahme eines Systemstandardwertes.	***SYSVAL** ***TYPEAHEAD** ***YES** ***NO**
OS400_Language Gibt die Sprachen-ID für dieses Benutzerprofil an.	***SYSVAL** *Sprachen-ID* Eine AS/400-Sprachen-ID
OS400_Limit_Cap Gibt an, ob die Funktionen dieses Benutzerprofils begrenzt werden sollen oder ob die Funktionen auf einen Systemstandardwert gesetzt werden sollen.	***PARTIAL** ***YES** ***NO**
OS400_Limit_Dev_Sess Gibt an, ob die Einheitensitzungen für diesen Benutzer begrenzt werden sollen oder ob ein Systemstandardwert übernommen werden soll.	***SYSVAL** ***YES** ***NO**
OS400_Locale Gibt den Pfadnamen der Ländereinstellung an, die der Umgebungsvariablen **LANG** zugeordnet ist. **Anmerkung:** Wird in Releases höher als V3R2 unterstützt.	***SYSVAL** ***NONE** ***C** ***POSIX** *Pfad* Ein durch "/" begrenzter Pfad für die Ländereinstellung
OS400_Loc_CCSID Gibt an, ob die CCSID der Ländereinstellung übernommen werden soll. **Anmerkung:** Wird in Releases höher als V3R2 unterstützt.	***YES** ***NO**

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_Loc_DATFMT Gibt an, ob das Datumsformat der Ländereinstellung verwendet werden soll. **Anmerkung:** Wird in Releases höher als V3R2 unterstützt.	***YES** ***NO**
OS400_Loc_DATSEP Gibt an, ob das Datumstrennzeichen der Ländereinstellung verwendet werden soll. **Anmerkung:** Wird in Releases höher als V3R2 unterstützt.	***YES** ***NO**
OS400_Loc_DECFMT Gibt an, ob das Dezimalformat der Ländereinstellung verwendet werden soll. **Anmerkung:** Wird in Releases höher als V3R2 unterstützt.	***YES** ***NO**
OS400_Loc_NONE Gibt an, ob der Wert **NONE** für Jobattribute, die der Ländereinstellung zugeordnet sind, gesetzt wird. **Anmerkung:** Wird in Releases höher als V3R2 unterstützt.	***YES** ***NO**
OS400_Loc_SRTSEQ Gibt an, ob die Sortierfolge der Ländereinstellung verwendet werden soll. **Anmerkung:** Wird in Releases höher als V3R2 unterstützt.	***YES** ***NO**
OS400_Loc_SYSVAL Gibt an, ob der Wert **SYSVAL** für Jobattribute, die der Ländereinstellung zugeordnet sind, gesetzt wird. **Anmerkung:** Wird in Releases höher als V3R2 unterstützt.	***YES** ***NO**

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_Loc_TIMSEP Gibt an, ob das Zeittrennzeichen der Ländereinstellung verwendet werden soll. **Anmerkung:** Wird in Releases höher als V3R2 unterstützt.	***YES** ***NO**
OS400_Login Gibt den Anmeldenamen des Benutzers an.	*Name* Eine Zeichenfolge mit 10 Zeichen oder weniger
OS400_Login_Enablement Gibt an, ob die Anmeldung des Benutzers möglich ist.	***ENABLED** ***DISABLED**
OS400_Login_Text Gibt die Beschreibung des Benutzerprofils in Textform an.	*Beschreibung* Eine Zeichenfolge mit 50 Zeichen oder weniger
OS400_Max_Storage Gibt den maximalen Zusatzspeicherplatz für permanente Objekte an.	***NOMAX** *Max_KB* Die zulässige Anzahl von Kilobytes
OS400_MSGQ Gibt die Nachrichtenwarteschlange an, die diesem Benutzer zugeordnet ist.	***USRPRF** *Warteschlangenname* Ein Warteschlangenname im Format LIB/QUEUE
OS400_MSG_Delivery Gibt an, wie die Nachrichten übermittelt werden. Diese Nachrichten werden an die Nachrichtenwarteschlangen gesendet, die dem Benutzerprofil zugeordnet sind.	***NOTIFY** ***HOLD** ***BREAK** ***DFT**
OS400_MSG_Sev_Level Gibt die niedrigste Bewertung für Nachrichten an, die dennoch an Benutzer im Zustellungsmodus **BREAK** oder **NOTIFY** gesendet werden.	*Bewertungscode* Eine ganze Zahl zwischen 0 und 99

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_Obj_Audit Gibt die Ebene der Objektverwendungsprotokollierung für diesen Benutzer an. **Anmerkung:** Dieses Attribute ist eine Schnittstelle zum Befehl **CHGUSRPRF**.	***NONE** ***CHANGE** ***ALL**
OS400_Obj_Create_Audit Gibt an, ob Protokolleinträge gesendet werden, wenn dieser Benutzer Objekte erstellt.	***YES** ***NO**
OS400_Obj_Delete_Audit Gibt an, ob Protokolleinträge gesendet werden, wenn dieser Benutzer Objekte löscht.	***YES** ***NO**
OS400_Obj_Mgmt_Audit Gibt an, ob Protokolleinträge gesendet werden, wenn dieser Benutzer Änderungen an der Objektverwaltung vornimmt und beispielsweise ein Objekt versetzt oder umbenennt.	***YES** ***NO**
OS400_Office_Audit Gibt an, ob Protokolleinträge gesendet werden, wenn dieser Benutzer Büroanwendungen ändert.	***YES** ***NO**
OS400_Optical_Audit Gibt an, ob bei Änderungen an optischen Einheiten Protokolleinträge gesendet werden. **Anmerkung:** Dieses Attribut wird nicht von V3R2 unterstützt; es wird ignoriert, wenn es an V3R2 weitergegeben oder verteilt wird.	***YES** ***NO**

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_OUTQ Gibt die Ausgabewarteschlange an, die diesem Benutzer zugeordnet ist.	***WRKSTN** ***DEV** *Warteschlangenname* Ein Warteschlangenname im Format LIB/QUEUE
OS400_Owner Gibt das OS/400-Benutzerprofil an, das Besitzer der neu erstellten Objekte ist.	***USRPRF** ***GRPPRF**
OS400_PassW Gibt das Kennwort an. Das Kennwort muss in der grafischen Benutzerschnittstelle (GUI) oder mit dem allgemeinen Benutzerkennwort in Tivoli explizit geändert werden. Während Weitergabevorgängen werden Kennwörter auf den Wert des Benutzerprofilnamens gesetzt.	*Kennwort* Eine Zeichenfolge mit 10 Zeichen oder weniger
OS400_PassW_Expired Gibt an, ob das Kennwort abgelaufen ist.	***YES** ***NO**
OS400_PassW_ExpInv Gibt das Ablaufintervall für das Kennwort an.	***SYSVAL** ***NOMAX** *Intervall* Eine ganze Zahl zwischen 1 und 366, die die Anzahl der Tage angibt, die zwischen einer Kennwortänderung und dessen Ablaufdatum liegen
OS400_PGM_Adopt_Audit Gibt an, ob Berechtigungen, die auf Grund von Programmübernahmen erteilt wurden, geprüft werden sollen.	***YES** ***NO**

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_Prim_GRP Gibt die Zugehörigkeit zu Primärgruppen an.	***NONE** *Gruppenname* Eine GRUPPE auf einem AS/400-Endpunkt. Der Name der GRUPPE muss bekannt sein, er kann nicht abgefragt werden.
OS400_Printer_Device Gibt den Namen des Standarddruckers an.	***WRKSTN** ***SYSVAL** *Name* Ein Drucker, der auf einem AS/400-Endpunkt definiert ist
OS400_Priority Gibt die höchste Prioritätsstufe für die Jobübergabe an.	*Zahl* Eine ganze Zahl zwischen 0 und 9
OS400_Priv_ALLOBJ Gibt an, ob die Berechtigung für den Zugriff auf Systemressourcen allen Objekten erteilt werden soll.	***YES** ***NO**
OS400_Priv_AUDIT Gibt an, ob Protokollierungsberechtigungen erteilt werden sollen.	***YES** ***NO**
OS400_Priv_IOSYSCFG Gibt an, ob Berechtigungen für die I/O-Konfiguration erteilt werden sollen.	***YES** ***NO**
OS400_Priv_JOBCTL Gibt an, ob Jobsteuerberechtigungen zum Ändern, Anzeigen, Anhalten, Freigeben, Abbrechen oder Löschen beliebiger aktiver Jobs erteilt werden sollen.	***YES** ***NO**

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_Priv_SAVSYS Gibt an, ob Berechtigungen zum Speichern, Wiederherstellen oder zum Freigeben von Speicherplatz für alle Systemobjekte erteilt werden sollen.	***YES** ***NO**
OS400_Priv_SECADM Gibt an, ob Sicherheitsverwaltungsberechtigungen zum Erstellen bzw. Ändern von Benutzerprofilen erteilt werden sollen.	***YES** ***NO**
OS400_Priv_SPLCTL Gibt an, ob Spool-Steuerungsberechtigungen erteilt werden sollen.	***YES** ***NO**
OS400_Priv_Service Gibt an, ob Dienstberechtigungen erteilt werden sollen.	***YES** ***NO**
OS400_Profile_Owner Gibt den Namen des OS/400-Benutzerprofils an, das der tatsächliche Besitzer des Objekts *USRPRF ist.	***NAME**
OS400_SAVRST_Audit Gibt an, ob Protokolleinträge für Speicher- und Wiederherstellungsvorgänge gesendet werden.	***YES** ***NO**
OS400_Security_Audit Gibt an, ob Protokolleinträge für Änderungen der Sicherheit gesendet werden.	***YES** ***NO**
OS400_Send_Message Gibt an, ob eine Nachricht an den Besitzer einer Spool-Datei gesendet wird, die anzeigt, dass der Druckvorgang beendet bzw. angehalten wurde.	***YES** ***NO**

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_Service_Audit Gibt an, ob Protokolleinträge für Systemdienste-Tools gesendet werden.	***YES** ***NO**
OS400_Show_Details Gibt an, ob zusätzliche Optionen angezeigt werden, wenn das System definiert bzw. geändert wird.	***YES** ***NO**
OS400_Show_Status_MSG Gibt an, ob Statusnachrichten gesendet werden.	***YES** ***NO**
OS400_Show_Parm_Keys Gibt an, ob bei der Anzeige eines Befehls Parameterschlüsselwörter an Stelle von möglichen Schlüsselwortwerten angezeigt werden.	***YES** ***NO**
OS400_Signon_Info Gibt an, ob Anmeldeinformationen angezeigt werden oder Systemstandardwerte verwendet werden.	***SYSVAL** ***YES** ***NO**
OS400_Sort_Sequence Gibt die Reihenfolge bei Zeichenfolgevergleichen an.	***SYSVAL** ***HEX** ***LANGIDUNK** ***LANGIDSHR** *Objekt* Ein Objekt im Format LIB/NAME
OS400_Special_Environment Gibt die Sonderumgebung an, in der der Benutzer arbeitet, nachdem er sich am System angemeldet hat.	***SYSVAL** ***NONE** ***S36**

AS/400-Attribute und Beschreibung	Schlüsselwortwerte
OS400_Spool_Audit Gibt an, ob Protokolleinträge für Spool-Dateioperationen, die von diesem Benutzer ausgeführt werden, gesendet werden.	***YES** ***NO**
OS400_Supp_GRPs Gibt zusätzliche Gruppenzugehörigkeiten an. **Anmerkung:** Wenn Sie mehrere zusätzliche Gruppen über die Befehlszeile angeben, müssen die Gruppen durch Kommas voneinander getrennt werden.	***NONE** *grp1 ... grpn* Eine Liste mit Gruppennamen. Bis zu 15 Gruppen können angegeben werden.
OS400_Sys_Mgmt_Audit Gibt an, ob Protokolleinträge für Aktionen zum Erteilen von Systemverwaltungsberechtigungen, die von diesem Benutzer ausgeführt werden, gesendet werden.	***YES** ***NO**
OS400_UID Gibt die AS/400-Benutzer-ID an.	***GEN** Eine vom System generierte ID *Zahl* Eine ganze Zahl zwischen 1 und 4294967294

OS/400-Benutzerkonten ändern

Verwenden Sie die folgenden Befehle, die von Tivoli SecureWay User Administration zum Ändern von OS/400-Attributen für Benutzerkonten zur Verfügung gestellt werden.

- Mit dem Befehl **wcrtusr** können Sie einen neuen Benutzer erstellen.
- Mit dem Befehl **wgetuser** können Sie Benutzerinformationen in einem vorhandenen Profil auflisten.
- Mit dem Befehl **wsetusr** können Sie Attribute in einem vorhandenen Benutzerprofil ändern.

In den folgenden Beispielen in diesem Abschnitt wird erläutert, wie Sie ein Tivoli-Profil für einen AS/400-Benutzer erstellen, Informationen zu diesem Profil abfragen und weitere Attribute für diesen Benutzer festlegen.

Mit dem Befehl **wcrtusr** können Sie einen neuen Benutzer in dem angegebenen Benutzerprofil erstellen. Beispiel: Wenn Sie ein Benutzerprofil für den Benutzer **nlloyd**, einen Mitarbeiter in Austin, Texas, erstellen möchten, geben Sie den Befehl **wcrtusr** ein, um den Benutzerdatensatz mit dem Namen des Mitarbeiters, der Telefonnummer und den Profilnamenattributen zu initialisieren.

```
wcrtusr -e 512-555-1212 -x OS400_Login NICK
        @UserProfile:Austin nlloyd
```

Dabei gilt Folgendes:

–e 512-555-1212
Gibt eine Durchwahlnummer an.

–x OS400_Login NICK
Setzt den Wert des OS/400-Attributnamens auf NICK.

@UserProfile:Austin
Gibt den Namen des Profils an, in dem der Benutzerdatensatz erstellt werden soll.

nlloyd Gibt den Namen des Profils an, in dem der Benutzerdatensatz erstellt werden soll.

Mit dem Befehl **wgetusr** werden Informationen zu einem bereits vorhandenen Benutzer im angegebenen Profil angezeigt. Wenn Sie beispielsweise eine Abfrage für das Attribut **OS400_DLT_Action** im AS/400-Benutzerprofil für **nlloyd** ausführen möchten, geben Sie den folgenden Befehl in der Befehlszeile ein:

```
wgetusr -x OS400_DLT_Action @UserProfile:Austin nlloyd
```

Dabei gilt Folgendes:

–x OS400_DLT_Action
Gibt den Wert des Attributs **OS400_DLT_Action** zurück.

@UserProfile:Austin
Gibt den Namen des Benutzerprofils an, für das eine Abfrage ausgeführt werden soll.

nlloyd Gibt den Anmeldenamen an.

Mit dem Befehl **wsetusr** können Sie die Attribute eines im angegebenen Benutzerprofil bereits vorhandenen Benutzers ändern. Wenn Sie beispielsweise den Wert des Attributs **OS400_DLT_Action** für die Benutzer **nlloyd** und **nmcginnis** festlegen möchten, geben Sie den folgenden Befehl in der Befehlszeile ein:

```
wsetusrs -x OS400_DLT_Action *DLT @UserProfile:Austin
         nlloyd nmcginnis
```

Dabei gilt Folgendes:

–x OS400_DLT_Action
Setzt den Wert des Attributs **OS400_DLT_Action**.

@UserProfile:Austin
Gibt den Namen des Benutzerprofils an, in dem die neuen Informationen festgelegt werden.

nlloyd nmcginnis
Gibt die Anmeldenamen an.

Weitere Informationen zum Erstellen und Ändern von Benutzerdatensätzen in Benutzerprofilen finden Sie im *Tivoli SecureWay User Administration Management Handbuch*. Weitere Informationen zur Befehlssyntax sowie zur Verwendung finden Sie im Handbuch *Tivoli SecureWay User Administration Reference Manual*.

B

OS/2-Benutzer verwalten

Tivoli SecureWay User Administration for OS/2 kann zusammen mit Tivoli SecureWay User Administration Version 3.8 in Unternehmensnetzwerken für die Verwaltung von Benutzerkonten und Benutzerkennwörtern eingesetzt werden. In Unternehmen, in denen mit verschiedenen Betriebssystemen und Anwendungsprogrammen gearbeitet wird, ermöglicht dieses Produkt über die Verwendung von Benutzerprofilen eine zentrale Verwaltung von Benutzerinformationen.

In diesem Kapitel werden Attribute für OS/2 sowie einige besondere Funktionen von Tivoli SecureWay User Administration for OS/2 auf OS/2-Endpunkten erläutert.

Vorteile einer Verwaltung von OS/2-Benutzerkonten über Tivoli

Momentan müssen Administratoren für die Verwaltung von OS/2-Benutzerkonten an einem OS/2-System angemeldet sein. Dadurch können nur die diesem System zugeordneten Benutzerkonten verwaltet werden. Darüber hinaus muss der Systemadministrator über gründliche Kenntnisse in Bezug auf die Verwaltung von OS/2-Benutzerkonten verfügen.

Nach der Installation von Tivoli SecureWay User Administration for OS/2 auf die vorhandene Installation von Tivoli SecureWay User Administration können Sie UNIX-, Windows NT-, NetWare- und OS/2-Benutzerkonten zentral verwalten. Damit wird die Zahl der

Benutzerschnittstellen verringert, mit denen Sie vertraut sein müssen, und die Konsistenz von Benutzerkonten unabhängig von der Kontoart sichergestellt.

Mit OS/2-Attributen und -Endpunkten arbeiten

Tivoli SecureWay User Administration for OS/2 ermöglicht Administratoren die Verwaltung von Benutzerkonten unter OS/2 Warp. Für alle Benutzerinformationen, die über die grafische OS/2-Benutzerschnittstelle verwaltet werden können, ist auch eine Verwaltung mit Hilfe von Tivoli SecureWay User Administration for OS/2 möglich. Bei einem OS/2-Endpunkt handelt es sich in der Regel um einen als Domänencontroller eingesetzten OS/2 Warp-Server mit TMA (Tivoli Management Agent), einem Softwaredienst für die Datenübertragung zwischen OS/2-Endpunkten und dem Gateway zum Tivoli-Server.

Für Vorgänge wie beispielsweise die Verteilung und Weitergabe an Domänencontroller ist die Anmeldung am OS/2-Zielsystem unter einem Administratorkonto erforderlich. Bei einer Verteilung empfängt ein Tivoli-Programm auf einem OS/2-Endpunkt Informationen, mit denen die Datenbank mit den OS/2-Benutzerkonten aktualisiert wird. Bei einer Weitergabe werden die in der OS/2-Datenbank mit Benutzerinformationen vorhandenen Daten vom OS/2 Warp-Server an ein angegebenes Benutzerprofil auf dem Tivoli-Server gesendet. Diese Funktion ist vor allem für die Datenweitergabe an neue Benutzerprofile mit OS/2-Benutzern hilfreich.

Unternehmen mit vielen OS/2 Warp-Servern verfügen unter Umständen über eine große Anzahl Domänen. Hier erweist es sich unter Umständen als vorteilhaft, wenn es sich bei den Domänen um Klone handelt. So können beispielsweise mit einem Benutzerprofil, das an viele Warp-Domänencontroller verteilt wird, in allen diesen Domänen identische Benutzerarten definiert werden, die jeweils über denselben Anmeldenamen, dasselbe Kennwort und weitere identische OS/2-Attribute verfügen. Bei der Weitergabe von Daten an ein neues Tivoli-Benutzerprofil hat es sich als vorteilhaft erwiesen, zunächst das Benutzerprofil zu erstellen und an dieses anschließend Daten aus OS/2-Benutzerkonten weiterzugeben.

OS/2-Benutzerattribute im Tivoli-Benutzerprofil

Bei der Installation werden dem Tivoli-Benutzerprofil folgende neue Bereiche hinzugefügt:

- **OS/2-Konto**
- **Optionen für OS/2-Konto**
- **Zuordnungen bei OS/2-Anmeldung**
- **Allgemeine OS/2-Anwendungen**
- **OS/2-Gruppenzugehörigkeit**
- **Anmelde-Workstations**

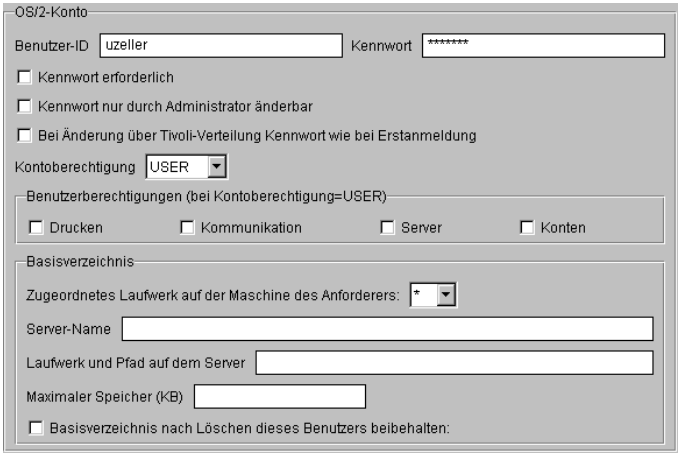
Diese OS/2-Bereiche sind im Dialog **Benutzermerkmale** enthalten. Die Attribute der einzelnen Bereiche werden in den folgenden Abschnitten erläutert. Sie können diese Attribute über die grafische Benutzerschnittstelle von Tivoli SecureWay User Administration anzeigen und bearbeiten.

Anmerkung: Die Verwendung dieser Attribute ist mit der Verwendung der Attribute für andere Endpunktarten in Tivoli SecureWay User Administration Version 3.8 identisch (falls nicht anders angegeben).

OS/2-Konto

Der Bereich **OS/2-Konto** enthält die allgemeinen Attribute für ein OS/2-Benutzerkonto.

1. Wählen Sie in der Merkmalliste die Option **OS/2-Konto** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Geben Sie im Feld **Benutzer-ID** den OS/2-Anmeldenamen des Benutzers ein. Diese ID darf nicht mit der UNIX-Benutzer-ID verwechselt werden, bei der es sich um eine Ganzzahl handelt.

   Der OS/2-Anmeldename wird separat von dem allgemeinen Anmeldenamen im Benutzerprofil gespeichert. Der OS/2-Anmeldename muss den OS/2-Namenskonventionen für Benutzer-IDs entsprechen. Der von Ihnen eingegebene Anmeldename wird vor der Verwendung vom OS/2-Endpunkt in Großbuchstaben umgesetzt, d. h., Sie können die Anmeldenamen im Tivoli-Benutzerprofil in Kleinbuchstaben speichern.

   Bei der Installation wird dem Profil für **Benutzer-ID** ein Skript für die Standardwertegruppe mit demselben Wert wie die allgemeine Anmelde-ID hinzugefügt. Es wird kein Gültigkeitsprüfungsskript für die Benutzer-ID zur Verfügung gestellt.

3. Geben Sie im Feld **Kennwort** das OS/2-Kennwort des Benutzers ein. Dieses Kennwort unterscheidet sich vom allgemeinen Kennwort und unterliegt den OS/2-Kennwortkonventionen.

   Bei der Installation wird dem Profil für **Benutzer-ID** ein Skript für die Standardwertegruppe mit demselben Wert wie das allgemeine Kennwort hinzugefügt. Es wird kein Gültigkeitsprüfungsskript für das Kennwort zur Verfügung gestellt.

4. Wählen Sie die Option **Kennwort erforderlich** aus, wenn für dieses Benutzerkonto auf dem OS/2-Zielsystem die Eingabe eines Kennworts erforderlich ist. Andernfalls ist die Angabe eines Kennworts optional.

5. Wählen Sie die Option **Kennwort nur durch Administrator änderbar** aus, wenn der Benutzer keine Möglichkeit erhalten soll, das eigene Kennwort mit den unter OS/2 zur Verfügung stehenden Funktionen zu ändern. In diesem Fall kann das Kennwort nur durch den Administrator oder durch Tivoli-Verteilungen geändert werden. Andernfalls können die Benutzer das Kennwort jederzeit unter OS/2 ändern.

6. Wenn Sie die Option **Bei Änderung über Tivoli-Verteilung Kennwort wie bei Erstanmeldung** aktivieren und das OS/2-Kennwort wurde geändert, läuft das geänderte Kennwort bei der nächsten Verteilung des Benutzerprofils ab. Damit kann sich der Benutzer zwar unter diesem Kennwort anmelden, er muss es aber anschließend sofort ändern. Gültig ist das nach der Änderung und der Verteilung festgelegte Kennwort.

7. Wählen Sie in der Dropdown-Liste **Kontoberechtigung** die gewünschte Berechtigung aus. Über diese Auswahl wird die Systemgruppe festgelegt, der der Benutzer zugeordnet wird. Mögliche Werte sind **GUEST**, **USER** und **ADMIN**.

   Wählen Sie bei Auswahl von USER im Bereich **Benutzerberechtigungen (bei Kontoberechtigung=USER)** die entsprechenden Optionen aus. (Bei Auswahl von **GUEST** oder **ADMIN** werden die Benutzerberechtigungen ignoriert.) Einzelheiten zu diesen Benutzerberechtigungen finden Sie in der Dokumentation zum OS/2 Warp-Server.

8. Geben Sie im Bereich **Basisverzeichnis** ein Laufwerk, einen Server und einen Verzeichnispfad an. Bei der Anmeldung eines Benutzers am OS/2 Warp-Server kann OS/2 das Laufwerk mit der Maschine des Anforderers verbinden, d. h., bei diesem handelt es sich um das Basisverzeichnis des Benutzers. Bei der Verteilung an den als primären Domänencontroller bzw. Backup-Domänencontroller eingesetzten OS/2 Warp-Server erstellt der Endpunkt das Basisverzeichnis und erteilt vollständigen Zugriff

darauf. Soll kein Basisverzeichnis angegeben werden, bleiben die Felder **Servername** und **Laufwerk und Pfad auf dem Server** leer.

Anmerkung: Die Angaben zum Basisverzeichnis werden nur verwendet, wenn es sich bei der Zielmaschine um einen primären bzw. Backup-Domänencontroller handelt.

Zugeordnetes Laufwerk auf der Maschine des Anforderers
Gibt den Laufwerkbuchstaben an, der auf der Maschine des Anforderers (d. h. auf der Workstation, von der aus sich der Benutzer angemeldet hat) bevorzugt für das Basisverzeichnis verwendet werden soll. Wählen Sie den Stern (*) aus; damit wird angegeben, dass als Basisverzeichnis der nächste verfügbare Laufwerkbuchstabe verwendet wird.

Servername
Gibt den Aliasnamen des Servers an, auf dem sich das Basisverzeichnis befindet. Die einem Servernamen normalerweise vorangestellten umgekehrten Schrägstriche (\\) dürfen hier nicht angegeben werden.

Laufwerk und Pfad auf dem Server
Gibt den vollständigen Pfad des Basisverzeichnisses auf dem Server im Format ***x*:*Pfad*** an; dabei steht *x* für den Laufwerkbuchstaben auf dem Server, gefolgt von einem Doppelpunkt, einem umgekehrten Schrägstrich und dem Basisverzeichnispfad.

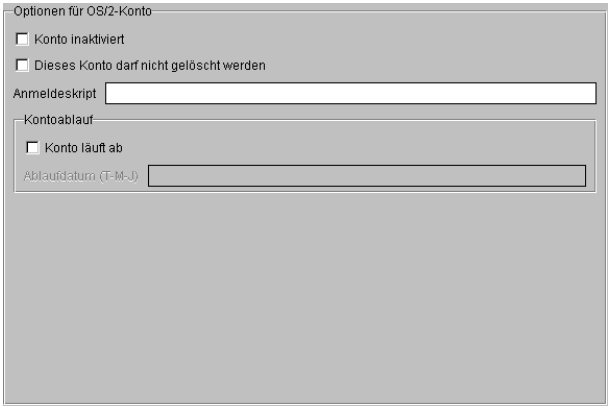
Maximaler Speicher (KB)
Die Angabe in diesem Feld ist optional. Hier können Sie die ungefähre maximale Speicherkapazität des Basisverzeichnisses in KB angeben. Informationen darüber, warum dieses Feld optional ist und keine Einschränkung durch den OS/2 Warp-Server besteht, finden Sie in der Dokumentation zum OS/2 Warp-Server.

Basisverzeichnis nach Löschen dieses Benutzers beibehalten
Aktivieren Sie dieses Kontrollkästchen, wenn das Basisverzeichnis nach dem Löschen des Benutzers beibehalten werden soll. Standardmäßig ist dieses Kontrollkästchen nicht aktiviert, d. h., beim Löschen des Benutzers wird das Basisverzeichnis ebenfalls gelöscht.

Optionen für OS/2-Konto

In der Anzeige **Optionen für OS/2-Konto** stehen mehrere neue Optionen zur Verfügung.

1. Wählen Sie in der Merkmalliste die Option **Optionen für OS/2-Konto** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Aktivieren Sie das Kontrollkästchen **Konto inaktiviert**, wenn das Konto nach der nächsten Tivoli-Verteilung inaktiviert werden soll. In diesem Fall kann sich der Benutzer nicht mehr unter der OS/2-Benutzer-ID anmelden. Andernfalls ist das Konto aktiviert.
3. Wird das Kontrollkästchen **Dieses Konto darf nicht gelöscht werden** aktiviert und anschließend ein Profil verteilt, kann das Konto auf dem OS/2 Warp-Server nicht gelöscht werden. Andernfalls kann dieses Konto entweder durch eine Tivoli-Verteilung oder durch den Administrator mit den auf dem OS/2 Warp-Server verfügbaren Funktionen gelöscht werden.

Tivoli SecureWay User Administration for OS/2 unterstützt die Verteilung exakter Kopien. Im Anschluss an eine solche Verteilung sind auf dem OS/2-Endpunkt nur die Benutzerkonten in den Profilen des Profilmanagers vorhanden. Alle übrigen Konten auf dem Endpunkt (mit Ausnahme derer, die vom Löschen ausgenommen wurden) werden gelöscht. Daher ist diese Option bei der Verteilung exakter Kopien eine gute Methode, um bestimmte Konten bei solchen Verteilungen vom Löschen auszunehmen.

Sie können Konten, die vom Löschen ausgenommen sind, trotzdem entfernen. Inaktivieren Sie dazu zunächst dieses Kontrollkästchen, und verteilen Sie das Profil; anschließend sollten Sie das Konto aus dem Benutzerprofil löschen und erneut verteilen.

4. Bei der Anmeldung eines Benutzers am OS/2 Warp-Server führt OS/2 für den Benutzer das im Feld **Anmeldeskript** angegebene Skript aus. Geben Sie den vollständigen Pfad und den Dateinamen des Anmeldeskripts ein. Soll kein Anmeldeskript ausgeführt werden, lassen Sie das Feld leer. Einzelheiten zu Anmeldeskripts finden Sie in der Dokumentation zum OS/2 Warp-Server.

5. Aktivieren Sie das Kontrollkästchen **Konto läuft ab**, wenn eine Gültigkeitsdauer für ein Konto angegeben werden soll. Das Konto wird daraufhin zu dem angegebenen Zeitpunkt inaktiviert. Das Datum wird im Format *T-J-J* angegeben.

   Anmerkung: Die Angabe führender Nullen für Tage und Monate ist nicht erforderlich. Tage, Monate und Jahre können durch Schrägstriche (/) getrennt werden.

Zuordnungen bei OS/2-Anmeldung

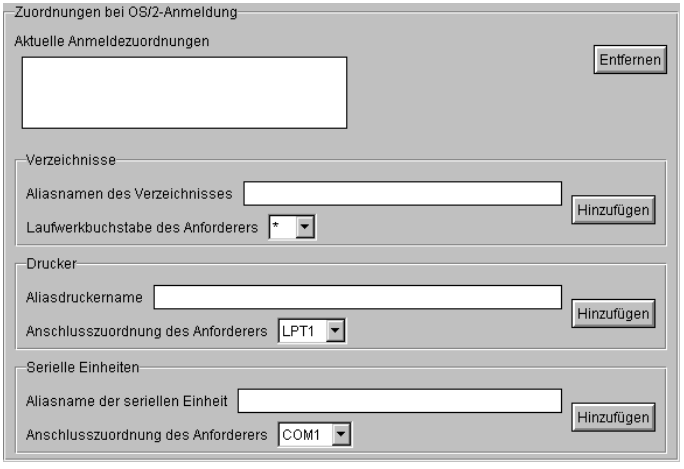
In der Anzeige **Zuordnungen bei OS/2-Anmeldung** stehen Optionen zur Verfügung, mit denen Benutzern bei der Anmeldung LAN-Ressourcen zugeordnet werden können.

Bei diesen Ressourcen kann es sich um Datenträger (oder Verzeichnisse, wie es in der OS/2-Terminologie heißt) oder serielle Einheiten wie Modems und Drucker handeln. Geben Sie in dieser Anzeige den Namen der LAN-Ressource ein, und geben Sie an, wie diese Ressource dem System des Anforderers zugeordnet werden soll.

Während einer Verteilung überprüft Tivoli das Vorhandensein der einzelnen Anmeldezuordnungen in der Zieldomäne. Wurde das Benutzerkonto definiert, wurden die Zuordnungen bei der Anmeldung für diesen Benutzer festgelegt. Wurde jedoch in der Zieldomäne kein Aliasname angegeben, wird dieser ignoriert. Dabei handelt es sich nicht um einen Fehler, und es werden auch keine entsprechenden Meldungen ausgegeben. Der Endpunkt versucht, alle für den Benutzer in der Zieldomäne angegebenen Anmeldezuordnungen hinzuzufügen.

In Tivoli sind maximal 100 zulässige Anmeldezuordnungen möglich.

1. Wählen Sie in der Merkmalliste die Option **Zuordnungen bei OS/2-Anmeldung** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. In der Liste **Aktuelle Anmeldezuordnungen** werden die dem Benutzerkonto zugeordneten Verzeichnisse, Drucker und seriellen Einheiten angezeigt. Zuordnungen können nicht durch direkte Eingabe in dieser Liste hinzugefügt werden. Sie können jedoch Einträge in dieser Liste auswählen, um sie zu bearbeiten oder zu löschen.

   Die Einträge in dieser Liste haben das Format *RESSOURCE-:EINHEIT*

   Dabei steht *RESSOURCE* für den im OS/2 Warp-Server definierten Aliasnamen der LAN-Ressource und *EINHEIT* gibt den Anschluss an, dem die Ressource bei der Anmeldung des Benutzers zugeordnet wird.

   Der Eintrag **INKJET:LPT3** beispielsweise gibt an, dass bei der Anmeldung der Drucker INKJET dem Anschluss LPT3 der Maschine des Anforderers zugeordnet wird. **PUBLICO:P** gibt an, dass das Verzeichnis PUBLICO bei der Anmeldung des Benutzers an das Laufwerk P: angehängt wird. **DATABASE:*** wiederum gibt an, dass die Ressource DATABASE dem nächsten verfügbaren Laufwerkbuchstaben auf der Maschine des Benutzers

zugewiesen wird, und **MODEM288:COM4** gibt an, dass die serielle Einheit MODEM288 dem Anschluss COM4 zugeordnet wird.

3. So fügen Sie der Liste der Anmeldezuordnungen einen Eintrag hinzu:

   a. Geben Sie den Aliasnamen der Ressource ein. OS/2-Aliasnamen werden in der Regel in Großbuchstaben eingegeben; da Kleinbuchstaben in Aliasnamen von den OS/2-Endpunkten jedoch generell in Großbuchstaben umgesetzt werden, kann die Angabe auch in Kleinbuchstaben erfolgen.

   b. Wählen Sie einen Laufwerkbuchstaben oder eine Einheit aus, dem bzw. der die LAN-Ressource auf dem System des Anforderers zugeordnet wird. Wenn Sie einen Stern (*) statt eines Laufwerkbuchstabens angeben, wird die Ressource an den nächsten verfügbaren Laufwerkbuchstaben auf dem System des Anforderers angehängt.

   c. Klicken Sie auf **Hinzufügen**. Der neue Eintrag wird daraufhin in der Liste mit Anmeldezuordnungen angezeigt.

Allgemeine OS/2-Anwendungen

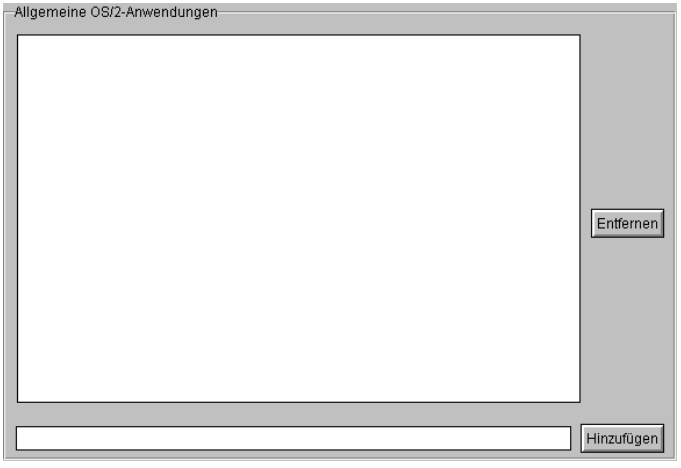
In der Anzeige **Allgemeine OS/2-Anwendungen** können Benutzer allgemeine und private Anwendungen zuweisen.

Bei der Anmeldung eines Benutzers an einer Workstation werden die allgemeinen Anwendungen in Form von Symbolen auf der Workstation-Arbeitsoberfläche angezeigt.

Von Tivoli werden nur allgemeine OS/2-Anwendungen unterstützt. Diese sollten bereits in der OS/2-Domäne definiert sein. Bei einer Verteilung versucht der Tivoli-OS/2-Endpunkt, für den Benutzer in der Zieldomäne so viele der vorhandenen Anwendungen wie möglich zu setzen. Falls die Liste Anwendungen enthält, die in der Domäne nicht definiert sind, so handelt es sich nicht um einen Fehler, und es werden auch keine entsprechenden Meldungen ausgegeben.

In Tivoli können einem Tivoli-Benutzerkonto maximal 100 allgemeine Anwendungen hinzugefügt werden.

1. Wählen Sie in der Merkmalliste die Option **OS/2-Anwendungen** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



2. Soll ein Eintrag aus der Liste entfernt werden, wählen Sie den betreffenden Eintrag aus, und klicken Sie anschließend auf **Entfernen**.
3. Soll der Liste mit allgemeinen Anwendungen ein neuer Eintrag hinzugefügt werden, geben Sie im Textfeld den Aliasnamen der Anwendung ein, und klicken Sie auf **Hinzufügen**.

OS/2-Gruppenzugehörigkeit

In der Anzeige **OS/2-Gruppenzugehörigkeit** kann ein Benutzer eine Liste mit den Namen der Gruppen zur Verfügung stellen, zu denen er gehört.

Bei der Verteilung fügt der OS/2-Endpunkt den Benutzer jeder der angegebenen Gruppen hinzu, die in der Zieldomäne zulässig sind, mit Ausnahme der folgenden vom System definierten Gruppen, die über das Attribut **Benutzerberechtigungen** vergeben werden: USERS, GUESTS, SERVERS, LOCAL und ADMINS. Die Option **Benutzerberechtigungen** ist in der Anzeige **OS/2-Konto** verfügbar. Bei Angabe einer Gruppe, die in der Zieldomäne nicht zulässig ist, handelt es sich nicht um einen Fehler, und es wird keine entsprechende Meldung ausgegeben.

Sie können einen Benutzer maximal 100 zulässigen Gruppen hinzufügen.

1. Wählen Sie in der Merkmalliste die Option **OS/2-Gruppenzugehörigkeit** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:

   Dieses Listenfenster enthält alle Gruppennamen, die für den Benutzer definiert sind. Gruppen können in Kleinbuchstaben eingegeben werden, da sie vom OS/2-Endpunkt vor der Verwendung in Großbuchstaben umgesetzt werden.

2. Soll ein Eintrag aus der Liste entfernt werden, wählen Sie den betreffenden Eintrag aus, und klicken Sie anschließend auf **Entfernen**.

3. Soll der Liste eine neue Gruppe hinzugefügt werden, geben Sie im Textfeld den Namen der Gruppe ein, und klicken Sie auf **Hinzufügen**.

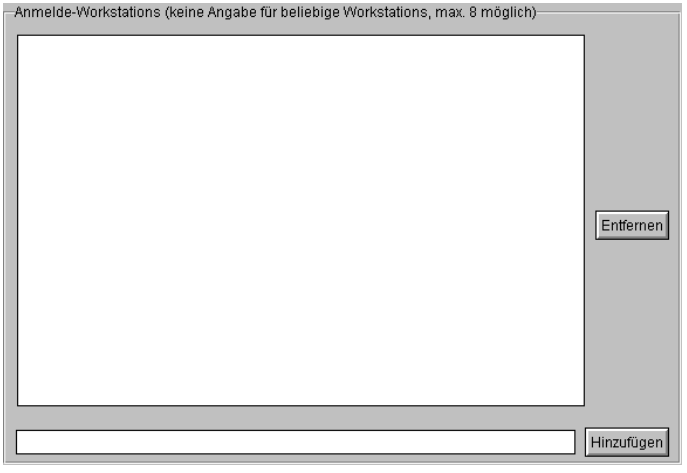
Anmelde-Workstations

In der Anzeige **Anmelde-Workstations** können Administratoren die Anmeldung von Benutzern auf bestimmte Workstations einschränken.

In dieser Anzeige können Sie bis zu acht Workstations eingeben, von denen aus sich ein Benutzer anmelden kann. Die angegebenen Workstation-Namen werden weder von Tivoli noch von OS/2 überprüft.

Anmerkung: Lassen Sie die Liste leer, wenn dem Benutzer ermöglicht werden soll, sich von jeder beliebigen Workstation aus anzumelden.

1. Wählen Sie in der Merkmalliste den Eintrag **OS/2-Anmelde-Workstations** aus, um Folgendes im Merkmalbereich des Dialogs **Benutzermerkmale** anzuzeigen:



   Dieses Listenfenster enthält die Namen der Workstations, von denen aus sich ein Benutzer anmelden kann. Angaben in Kleinbuchstaben sind möglich, da diese vom Endpunkt in Großbuchstaben umgesetzt werden.

2. Soll ein Eintrag aus der Liste entfernt werden, wählen Sie den betreffenden Eintrag aus, und klicken Sie anschließend auf **Entfernen**.

3. Soll der Liste eine neue Workstation hinzugefügt werden, geben Sie im unteren Textfeld den Namen der Workstation ein, und klicken Sie auf **Hinzufügen**.

   Lassen Sie die Liste leer, wenn der Benutzer die Möglichkeit haben soll, sich von jeder beliebigen Workstation aus anzumelden.

Funktionsweise von SecureWay User Administration auf OS/2-Endpunkten

In den folgenden Abschnitten wird beschrieben, wie Tivoli SecureWay User Administration mit dem Tivoli SecureWay User Administration for OS/2-Endpunktagenten arbeitet.

OS/2-Endpunkt als primärer bzw. Backup-Domänencontroller

In einer typischen Installation werden von Tivoli Benutzerdaten an einen als primären Domänencontroller eingesetzten OS/2 Warp-Server verteilt bzw. aus diesem übernommen. Der Tivoli-Agent auf einem OS/2-Endpunkt arbeitet dabei mit der lokalen Benutzerkontendatenbank. Da es sich bei diesem System um einen primären Domänencontroller handelt, handelt es sich bei der lokalen Benutzerkontendatenbank um die Benutzerdatenbank der LAN-Domäne.

Alternativ dazu kann Tivoli Benutzerdaten auch an den Backup-Domänencontroller verteilen bzw. aus diesem übernehmen. In diesem Fall handelt es sich bei der Zieldatenbank ebenfalls um die Benutzerdatenbank der LAN-Domäne. Alle Anforderungen an den Backup-Domänencontroller werden einfach an den Domänencontroller weitergeleitet. Daher sollte als Tivoli-Zieladresse entweder der primäre Domänencontroller oder der Backup-Domänencontroller ausgewählt werden, nicht aber beide.

Unabhängig von dem angegebenen Controller ist auf jeden Fall die Anmeldung als OS/2-Administrator erforderlich. Wenn es sich bei der Zielmaschine um den primären oder Backup-Domänencontroller handelt, muss die Anmeldung auf der Zielmaschine unter einem Konto mit Administratorberechtigung erfolgen. Erfolgt keine Anmel-

dung oder handelt es sich bei dem Anmelder nicht um einen Administrator, wird der Vorgang vom dem Tivoli-Agenten unter OS/2 umgehend abgebrochen.

Verteilung an andere OS/2-Server und -Systeme

Die OS/2 Warp-Serverumgebung umfasst auch mehrere normale Server. Dabei handelt es sich um zusätzliche Server in der Domäne, die weder als primäre noch als Backup-Domänencontroller dienen.

Wird ein solcher Server als Ziel einer Tivoli-Operation angegeben, ist nur die lokale Benutzerkontendatenbank auf diesem Server bei diesem Vorgang betroffen. Es wird weder das Basisverzeichnis verarbeitet, noch ist für den Vorgang die Anmeldung unter einem Administratorkonto erforderlich.

Die DB/2-Datenbank für OS/2 führt eine Authentifizierung der Benutzer anhand der lokalen Benutzerkontendatenbank durch. Einige Tivoli-Kunden setzen DB/2-Server für die Verwaltung der DB/2-Benutzer in dieser lokalen Benutzerdatenbank ein.

Als Zielsystem können für Tivoli auch Systeme angegeben werden, bei denen es sich nicht um Server handelt. Der Tivoli-Endpunktagent kann auf jedem OS/2-System mit einer lokalen Benutzerkontendatenbank zum Einsatz kommen. Alle Tivoli-Vorgänge wirken sich auf die lokale Benutzerkontendatenbank auf dem jeweiligen System aus.

Für die Benutzerverwaltung auf dem OS/2-Endpunkt durch den Tivoli-Agenten unter OS/2 ist unter anderem die Bibliothek **NETAPI32.DLL** erforderlich.

Benutzer ohne Kennwort

Ein Benutzer, der ein Attribut festlegt, für das ein Kennwort erforderlich (**TRUE**) ist, jedoch über kein Kennwort verfügt, werden bei einer Verteilung umgehend zurückgewiesen. Es erfolgt keine weitere Verarbeitung für diesen Datensatz im Benutzerprofil, sondern die Verteilung wird mit dem nächsten Benutzer im Benutzerprofil fortgesetzt. Vom Endpunkt wird eine entsprechende Meldung an das Schwarze Brett (Bulletin Board) gesendet.

Anmerkung: Sie können das Schwarze Brett anzeigen, indem Sie auf das entsprechende Symbol auf der Tivoli-Arbeitsoberfläche klicken.

Benutzer mit geändertem Kennwort

Tivoli ändert das Kennwort unter OS/2 nur, wenn das Kennwort im Benutzerprofil vor einer Verteilung geändert wurde. Diese Markierung wird nach einer Verteilung zurückgenommen, bis sie im Benutzerprofil von einem Tivoli-Administrator erneut aktiviert wird. OS/2-Benutzer können ihre Kennwörter mit der entsprechenden OS/2-Funktion ändern; die geänderten Kennwörter werden auch von einer nachfolgenden Tivoli-Verteilung nicht überschrieben.

Benutzer mit geänderter Benutzer-ID (Anmeldename)

Beim Ändern einer OS/2-Benutzer-ID muss berücksichtigt werden, dass die alte Benutzer-ID nach Erstellung der neuen Benutzer-ID nach wie vor auf dem Endpunkt vorhanden ist. Dies bedeutet, dass zwei Konten anstatt eines geänderten Kontos vorliegen. Im Endpunkt selbst kann nach dem Ändern einer Benutzer-ID nicht mehr festgestellt werden, wie der alte Wert lautet.

Dieses Problem kann wie folgt vermieden werden:

1. Löschen Sie zunächst den Benutzer aus dem Benutzerprofil.
2. Verteilen Sie das Benutzerprofil.
3. Fügen Sie den Benutzer dem Benutzerprofil unter einer neuen Benutzer-ID hinzu.
4. Verteilen Sie das Benutzerprofil erneut.

Benutzer in der OS/2-Gruppe 'SERVERS'

Unter OS/2 wird für jeden OS/2-Server in der Domäne ein Benutzerkonto geführt. Diese Konten stehen nicht für Personen, sondern gehören zur Gruppe **SERVERS**. Konten, die zu dieser Gruppe gehören, werden von Tivoli weder gelöscht noch bei einer Weitergabe an ein Benutzerprofil weitergegeben.

OS/2-Attributnamen in Benutzerprofilen

Die folgenden Attribute wurden Tivoli SecureWay User Administration zur Verwendung mit den Befehlen **wgetusr** und **wsetusr** hinzugefügt. Diese Attribute sind vor allem für OS/2-Endpunkte bestimmt und können dazu verwendet werden, Ihr System über die Befehlszeilenschnittstelle zu verwalten. Im Handbuch *Tivoli SecureWay User Administration Reference Manual* finden Sie alle Informationen zur Verwendung der Befehle **wgetusr** und **wsetusr** einschließlich einer Liste mit allen anderen verfügbaren Attribute.

Anmerkung: In dieser Liste sind die tatsächlichen Namen der Attribute aufgeführt, die für die Verwaltung der OS/2-Umgebung verwendet werden. Diese Namen werden nicht auf der grafischen Benutzerschnittstelle von Tivoli SecureWay User Administration angezeigt, jedoch müssen sie beispielsweise bei der Verwendung der Befehle **wgetusr** und **wsetusr** dem Argument **–x** folgen. Beispiel:

```
wgetusr -x os2_applications
```

os2_applications Eine Liste mit Aliasnamen für allgemeine Anwendungen (jeweils durch ein Komma voneinander getrennt), die diesem Benutzer zugeordnet sind.

os2_groups Eine Liste mit Gruppennamen (jeweils durch ein Komma voneinander getrennt), die diesem Benutzer zugeordnet sind.

os2_homedir_assigned_drive Entweder ein Laufwerkbuchstabe (nur der Buchstabe, kein Doppelpunkt) oder ein Stern (*). Hierbei handelt es sich um das Laufwerk, auf dem das Basisverzeichnis dem Anforderer zugeordnet wird, wenn sich der Benutzer am OS/2 WARP-Server anmeldet. In diesem Feld darf nur ein Zeichen eingegeben werden.

os2_homedir_server_name	Der Name des Servers, auf dem sich das Basisverzeichnis des Benutzers befindet. Vor dem Servernamen dürfen keine umgekehrten Schrägstriche (\\) eingegeben werden. Lassen Sie das Feld leer, wenn Sie kein Basisverzeichnis zuordnen möchten.
os2_homedir_server_path	Das Laufwerk und der vollständige Pfad für das Basisverzeichnis des Benutzers auf dem Server. Das hier angegebene Laufwerk befindet sich auf dem Server und nicht auf der Maschine des Anforderers. Lassen Sie das Feld leer, wenn Sie kein Basisverzeichnis zuordnen möchten.
os2_homedir_keep	Ein Boolescher Wert, der angibt, was mit einem Benutzerbasisverzeichnis beim Löschen dieses Benutzers geschieht. Der Wert 'FALSE' bedeutet, dass das Basisverzeichnis entfernt wird, wenn der Benutzer gelöscht wird. Der Wert 'TRUE' bedeutet, dass das Basisverzeichnis bestehen bleibt, wenn der Benutzer gelöscht wird. Geben Sie **Yes** oder **1** für den Wert 'TRUE' und **No** oder **0** für den Wert 'FALSE' an.
os2_logon_script	Der vollständig qualifizierte Pfad und Dateiname des Benutzeranmeldeskripts. Lassen Sie das Feld leer, wenn Sie kein Anmeldeskript zuordnen möchten.
os2_logon_assignments	Eine Liste mit Anmeldezuordnungen, die jeweils durch ein Komma voneinander getrennt sind. Jede Anmeldezuordnung hat das Format *RESSOURCE*:*EINHEIT*, wobei *RES-*

	SOURCE der Aliasname der Ressource in der Domäne ist, und *EINHEIT* beschreibt, wie diese Ressource eine Verbindung zum Anforderer herstellt, wenn sich der Benutzer anmeldet. Wenn es sich um eine Plattenressource handelt, können Sie für *EINHEIT* einen Stern (*****) für den nächsten verfügbaren Laufwerkbuchstaben bzw. einen Buchstaben von D bis Z eingeben. Für serielle Einheiten können Sie für *EINHEIT* COM1, COM2, COM3, ... COM9 eingeben. Ist die Ressource ein Drucker, kann für *EINHEIT* LPT1, LPT2, ... LPT9 eingegeben werden.
os2_max_storage	Eine ganze Zahl (in KB), die OS/2 die maximale Speichergrenze für ein Benutzerbasisverzeichnis anzeigt. Lassen Sie das Feld leer, wenn Sie keine Speichergrenze zuordnen möchten.
os2_userpriv_print	Ein Boolescher Wert, der den Benutzern die Steuerung gemeinsamer Druckwarteschlangen für den lokalen Server ermöglicht. Geben Sie **Yes** oder **1** für den Wert 'TRUE' und **No** oder **0** für den Wert 'FALSE' an.
os2_userpriv_comm	Ein Boolescher Wert, der den Benutzern die Steuerung gemeinsamer Warteschlangen für DFV-Einheiten für den lokalen Server ermöglicht. Geben Sie **Yes** oder **1** für den Wert 'TRUE' **No** oder **0** für den Wert 'FALSE' an.
os2_userpriv_server	Ein Boolescher Wert, der den Benutzern die Steuerung gemeinsamer

	Ressourcen für den lokalen Server ermöglicht. Geben Sie **Yes** oder **1** für den Wert 'TRUE' **No** oder **0** für den Wert 'FALSE' an.
os2_userpriv_accounts	Ein Boolescher Wert, der den Benutzern die Steuerung anderer Benutzerkonten und -gruppen in der Domäne ermöglicht. Geben Sie **Yes** oder **1** für den Wert 'TRUE' **No** oder **0** für den Wert 'FALSE' an.
os2_password	Ein verschlüsselter Wert. Hierbei kann es sich um eine Kopie des verschlüsselten allgemeinen Kennworts handeln (Kennwort für Einzelanmeldung).
os2_password_required	Ein Boolescher Wert, der ein Kennwort für den OS/2 WARP-Server erforderlich macht. Geben Sie **Yes** oder **1** für den Wert 'TRUE' und **No** oder **0** für den Wert 'FALSE' an.
os2_password_admin_only	Ein Boolescher Wert, der es einem Administrator bzw. einer Tivoli-Verteilung ermöglicht, nur das Kennwort des Benutzerkontos zu ändern. Geben Sie **Yes** oder **1** für den Wert 'TRUE' **No** oder **0** für den Wert 'FALSE' an.
os2_password_preexpire	Ein Boolescher Wert, durch den das neu geänderte Kennwort bei Verteilung des Benutzerprofils sofort abläuft. Geben Sie **Yes** oder **1** für den Wert 'TRUE' **No** oder **0** für den Wert 'FALSE' an.

os2_privilege	Mögliche Werte sind **USER**, **GUEST** bzw. **ADMIN**. *Hier ist die Eingabe von Großbuchstaben erforderlich.*
os2_userid	Die OS/2-Benutzer-ID bzw. der Anmeldename.
os2_account_expires	Ein Boolescher Wert, der angibt, ob ein Konto ablaufen wird. Das Attribut **os2_account_expiration_date** gibt das Ablaufdatum an. Der Wert **FALSE** zeigt an, dass das Konto niemals abläuft. Geben Sie **Yes** oder **1** für den Wert 'TRUE' und **No** oder **0** für den Wert 'FALSE' an.
os2_account_expiration_date	Ein Datum im Format *TT-MM-JJJJ*. Bei der Angabe des Tages und des Monats sind keine führenden Nullen erforderlich. Tage, Monate und Jahre können durch Schrägstriche (/) und Silbentrennungsstriche (-) getrennt werden.
os2_account_disabled	Ein Boolescher Wert, der angibt, ob ein Benutzerkonto inaktiviert ist. Geben Sie **Yes** oder **1** für den Wert 'TRUE' und **No** oder **0** für den Wert 'FALSE' an.
os2_delete_prohibited	Ein Boolescher Wert, der angibt, dass das Konto nicht gelöscht werden kann. Der Wert TRUE bedeutet, dass das Konto nicht gelöscht werden kann. Der Wert FALSE bedeutet, dass das Konto gelöscht werden kann. Geben Sie **Yes** oder **1** für den Wert 'TRUE' und **No** oder **0** für den Wert 'FALSE' an.

os2_workstations	Eine Liste mit Namen von Workstations (Anforderer), die jeweils durch ein Komma voneinander getrennt sind, von denen aus sich ein Benutzer am OS/2 WARP-Server anmelden kann.
real_name	Der tatsächliche Name des Benutzers, der sowohl den Vornamen als auch den Nachnamen beinhaltet. Tivoli-Endpunkte verwenden dieses Attribut, um ein ähnliches Attribut für den OS/2 WARP-Server festzulegen. Verwenden Sie für die Angabe des tatsächlichen Namens die Befehle **wgetusr** und **wsetusr** mit der Option **-R**, nicht mit der Option **-x**.

OS/2-Ergebniscodes

Während der Verteilungsvorgänge gibt Tivoli unerwartete Fehlercodes von den OS/2 WARP-Anwendungsprogrammierschnittstellen (APIs) zurück. Das Endpunktprogramm schreibt Nachrichten in die Tivoli **Hinweise** in der Kategorie 'Benutzerverwaltung'. Sie können die Nachrichten anzeigen, indem Sie auf das Symbol **Hinweise** auf der Tivoli-Arbeitsoberfläche klicken.

Anmerkung: Es wird empfohlen, dass den Administratoren, die mit Tivoli SecureWay User Administration arbeiten, Berechtigungen für die Verwendung der Benutzerverwaltungshinweise erteilt werden.

Die folgende Liste mit Ergebniscodes für Net32*-API wurde der Datei **neterr.h** entnommen. Die Zahlen sind Dezimalzahlen.

Fehler	Definition	Anmerkungen
2	DATEI WURDE NICHT GEFUNDEN	Die Datei wurde nicht gefunden.
3	PFAD NICHT GEFUNDEN	Der Pfad wurde nicht gefunden.
5	ZUGRIFF VERWEIGERT	Administratorberechtigungen sind erforderlich.
50	ERROR_NOT_SUPPORTED	Die Netzwerkanforderung wird nicht unterstützt.
51	ERROR_REM_NOT_LIST	Dieser ferne Computer ist nicht empfangsbereit.
52	ERROR_DUP_NAME	Auf dem Netzwerk ist ein identischer Name vorhanden.
53	ERROR_BAD_NETPATH	Der Netzwerkpfad wurde nicht gefunden.
54	ERROR_NETWORK_BUSY	Das Netzwerk ist ausgelastet.
55	ERROR_DEV_NOT_EXIST	Die angegebene Einheit ist nicht im Netzwerk vorhanden.
56	ERROR_TOO_MANY_CMDS	Die Befehlsbegrenzung auf dem Netzwerk-BIOS wurde erreicht.
57	ERROR_ADAP_HDW_ERR	Im Netzwerkadapter ist ein Hardwarefehler aufgetreten.
58	ERROR_BAD_NET_RESP	Die Antwort des Netzwerks ist ungültig.
59	ERROR_UNEXP_NET_ERR	Ein unerwarteter Netzwerkfehler ist aufgetreten.
60	ERROR_BAD_REM_ADAP	Der ferne Adapter ist nicht kompatibel.

Fehler	Definition	Anmerkungen
61	ERROR_PRINTQ_FULL	Die Druckwarteschlange ist voll.
62	ERROR_NO_SPOOL_SPACE	Auf dem Server ist nicht genügend Speicherplatz zum Speichern der Datei, die gedruckt werden soll, vorhanden.
63	ERROR_PRINT_CANCELLED	Die angeforderte Druckdatei wurde abgebrochen.
64	ERROR_NETNAME_DELETED	Der Netzwerkname wurde gelöscht.
65	ERROR_NETWORK_ACCESS_DENIED	Der Zugriff auf das Netzwerk wurde verweigert.
66	ERROR_BAD_DEV_TYPE	Die Netzwerk-Ressourcenart ist ungültig.
67	ERROR_BAD_NET_NAME	Der Netzwerkname wurde nicht gefunden.
68	ERROR_TOO_MANY_NAMES	Die Namensbegrenzung für die Adapterkarte des lokalen Computernetzwerks wurde überschritten.
69	ERROR_TOO_MANY_SESS	Die Sitzungsbegrenzung für das Netzwerk-BIOS wurde überschritten.
70	ERROR_SHARING_PAUSED	Gemeinsamer Dateizugriff wurde vorübergehend angehalten.
71	ERROR_REQ_NOT_ACCEP	Die Netzwerkanforderung wurde abgelehnt.
72	ERROR_REDIR_PAUSED	Die Druck- bzw. Datenträgerumleitung wurde vorübergehend angehalten.
87	ERROR_INVALID_PARAMETER	Die Parameter sind ungültig.
88	ERROR_NET_WRITE_FAULT	In den Netzwerkdaten ist ein Fehler aufgetreten.
230	ERROR_BAD_PIPE	Hierbei handelt es sich um eine nicht vorhandene Pipe oder eine ungültige Operation.
231	ERROR_PIPE_BUSY	Die angegebene Pipe ist ausgelastet.
232	ERROR_NO_DATA	Bei einem nicht geblockten Lesevorgang können keine Daten gelesen werden.
233	ERROR_PIPE_NOT_CONNECTED	Der Server hat die Verbindung zur Pipe getrennt.
234	ERROR_MORE_DATA	Zusatzdaten sind verfügbar.
240	ERROR_VC_DISCONNECTED	Die Sitzung wurde abgebrochen.
2102	NERR_NetNotStarted	Der Treiber **NETWKSTA.SYS** für die Workstation wurde nicht installiert.
2103	NERR_UnknownServer	Der Server wurde nicht gefunden.

Fehler	Definition	Anmerkungen
2104	NERR_ShareMem	Ein interner Fehler ist aufgetreten. Das Netzwerk konnte nicht auf ein Segment eines gemeinsam benutzten Speichers zugreifen.
2105	NERR_NoNetworkResource	Es sind nicht genügend Netzwerkressourcen vorhanden.
2106	NERR_RemoteOnly	Diese Operation wird nicht für Workstations unterstützt.
2107	NERR_DevNotRedirected	Es besteht keine Verbindung zu der Einheit.
2114	NERR_ServerNotStarted	Der Serverdienst wurde nicht gestartet.
2115	NERR_ItemNotFound	Die Warteschlange ist leer.
2116	NERR_UnknownDevDir	Die Einheit oder das Verzeichnis ist nicht vorhanden.
2117	NERR_RedirectedPath	Die Operation ist für eine umgeleitete Ressource ungültig.
2118	NERR_DuplicateShare	Der Name wird bereits gemeinsam benutzt.
2119	NERR_NoRoom	Der Server verfügt momentan nicht über die angeforderte Ressource.
2121	NERR_TooManyItems	Die Anforderung, ein Element hinzuzufügen, überschreitet das zulässige Maximum.
2122	NERR_InvalidMaxUsers	Der Peer-Dienst unterstützt nur zwei simultane Benutzer.
2123	nNERR_BufTooSmall	Der API-Rückgabepuffer ist zu klein.
2127	NERR_RemoteErr	Ein ferner API-Fehler ist aufgetreten.
2131	NERR_LanmanIniError	Beim Öffnen bzw. Lesen der Datei **IBMLAN.INI** ist ein Fehler aufgetreten.
2134	NERR_OS2IoctlError	Beim Aufruf des Workstation-Treibers ist ein interner Fehler aufgetreten.
2136	NERR_NetworkError	Ein allgemeiner Netzwerkfehler ist aufgetreten.
2138	NERR_WkstaNotStarted	Der Requester-Dienst wurde nicht gestartet.
2140	NERR_InternalError	Ein interner LAN-Manager-Fehler ist aufgetreten.
2141	NERR_BadTransactConfig	Der Server wurde nicht für Transaktionen konfiguriert.
2142	NERR_InvalidAPI	Die angeforderte API wird nicht vom fernen Server unterstützt.
2143	NERR_BadEventName	Der Ereignisname ist ungültig.

Fehler	Definition	Anmerkungen
2146	NERR_CfgCompNotFound	Die angegebene Komponente konnte in der Datei **IBMLAN.INI** nicht gefunden werden.
2147	NERR_CfgParamNotFound	Der angegebene Parameter konnte in der Datei **IBMLAN.INI** nicht gefunden werden.
2149	NERR_LineTooLong	Eine Zeile in der Datei **IBMLAN.INI** ist zu lang.
2150	NERR_QNotFound	Die Druckwarteschlange ist nicht vorhanden.
2151	NERR_JobNotFound	Der Druckjob ist nicht vorhanden.
2152	NERR_DestNotFound	Die Druckerzieladresse wurde nicht gefunden.
2153	NERR_DestExists	Die Druckerzieladresse ist bereits vorhanden.
2154	NERR_QExists	Die Druckwarteschlange ist bereits vorhanden.
2155	NERR_QNoRoom	Es können keine weiteren Druckwarteschlangen hinzugefügt werden.
2156	NERR_JobNoRoom	Es können keine weiteren Druckjobs hinzugefügt werden.
2157	NERR_DestNoRoom	Es können keine weiteren Druckerzieladressen hinzugefügt werden.
2158	NERR_DestIdle	Diese Druckerzieladresse ist inaktiv und kann keine Steueroperationen akzeptieren.
2159	NERR_DestInvalidOp	Diese Anforderung an die Druckerzieladresse enthält eine ungültige Steuerfunktion.
2160	NERR_ProcNoRespond	Der Druckerprozessor antwortet nicht.
2161	NERR_SpoolerNotLoaded	Der Spooler ist nicht aktiv.
2162	NERR_DestInvalidState	Die angegebene Operation kann wegen des momentanen Status der Ausgabeeinheit nicht ausgeführt werden.
2163	NERR_QInvalidState	Die angegebene Operation kann wegen des momentanen Status der Druckwarteschlange nicht ausgeführt werden.
2164	NERR_JobInvalidState	Die angegebene Operation kann wegen des momentanen Status des Druckjobs nicht ausgeführt werden.
2165	NERR_SpoolNoMemory	Bei der Zuordnung von Speicherplatz an den Spooler ist ein Fehler aufgetreten.

Fehler	Definition	Anmerkungen
2166	NERR_DriverNotFound	Der Einheitentreiber ist nicht vorhanden.
2167	NERR_DataTypeInvalid	Der Datentyp wird vom Prozessor nicht unterstützt.
2168	NERR_ProcNotFound	Der Druckprozessor ist nicht installiert worden.
2180	NERR_ServiceTableLocked	Der Dienst reagiert nicht auf Steuerungsaktionen.
2181	NERR_ServiceTableFull	Die Diensttabelle ist voll.
2182	NERR_ServiceInstalled	Der angeforderte Dienst wurde bereits gestartet.
2183	NERR_ServiceEntryLocked	Der Dienst reagiert nicht auf Steuerungsaktionen.
2184	NERR_ServiceNotInstalled	Der Dienst wurde nicht gestartet.
2185	NERR_BadServiceName	Der Dienstname ist ungültig.
2186	NERR_ServiceCtlTimeout	Der Dienst reagiert nicht auf Steuerfunktionen.
2187	NERR_ServiceCtlBusy	Die Dienststeuerung ist ausgelastet.
2188	NERR_BadServiceProgName	**IBMLAN.INI** enthält einen ungültigen Dienstprogrammnamen.
2189	NERR_ServiceNotCtrl	Der Dienst kann wegen des aktuellen Status nicht gesteuert werden.
2190	NERR_ServiceKillProc	Der Dienst wurde abnormal beendet.
2191	NERR_ServiceCtlNotValid	Die angeforderte Pause bzw. der angeforderte Stopp ist für diesen Dienst ungültig.
2200	NERR_AlreadyLoggedOn	Diese Workstation ist bereits am lokalen Netzwerk angemeldet.
2201	NERR_NotLoggedOn	Diese Workstation wurde nicht am lokalen Netzwerk angemeldet.
2202	NERR_BadUsername	Der Benutzernamen- bzw. Gruppennamenparameter ist ungültig.
2203	NERR_BadPassword	Der Kennwortparameter ist ungültig.
2204	NERR_UnableToAddName_W	Der Anmeldeprozessor hat den Nachrichtenaliasnamen nicht hinzugefügt.
2205	NERR_UnableToAddName_F	Der Anmeldeprozessor hat den Nachrichtenaliasnamen nicht hinzugefügt.
2206	NERR_UnableToDelName_W	Der Abmeldeprozessor hat den Nachrichtenaliasnamen nicht gelöscht.
2207	NERR_UnableToDelName_F	Der Abmeldeprozessor hat den Nachrichtenaliasnamen nicht gelöscht.
2209	NERR_LogonsPaused	Netzwerkanmeldungen wurden angehalten.

Fehler	Definition	Anmerkungen
2210	NERR_LogonServerConflict	Ein zentraler Anmeldeserverkonflikt ist aufgetreten.
2212	NERR_LogonScriptError	Beim Laden oder Ausführen des Anmeldeskripts ist ein Fehler aufgetreten.
2214	NERR_StandaloneLogon	Es wurde kein Anmeldeserver angegeben. Ihr Computer wird als **STANDALONE** angemeldet.
2215	NERR_LogonServerNotFound	Der Anmeldeserver wurde nicht gefunden.
2217	NERR_NonValidatedLogon	Der Anmeldeserver konnte die Anmeldung nicht überprüfen.
2218	NERR_AccountUndeletable	Das Benutzerkonto wurde als nicht löschbar definiert.
2219	NERR_ACFNotFound	Die Abrechnungsdatei **NET.ACC** wurde nicht gefunden.
2220	NERR_GroupNotFound	Der Gruppenname wurde nicht gefunden.
2221	NERR_UserNotFound	Der Benutzername wurde nicht gefunden.
2222	NERR_ResourceNotFound	Der Ressourcenname wurde nicht gefunden.
2223	NERR_GroupExists	Die Gruppe ist bereits vorhanden.
2224	NERR_UserExists	Das Benutzerkonto ist bereits vorhanden.
2225	NERR_ResourceExists	Die Liste mit den Ressourcenberechtigungen ist bereits vorhanden.
2226	NERR_NotPrimary	Die UAS-Datenbank ist eine Kopie der Datenbank und ist daher nicht aktualisiert.
2227	NERR_ACFNotLoaded	Das Benutzerkontensystem wurde nicht gestartet.
2228	NERR_ACFNoRoom	Das Benutzerkontensystem enthält zu viele Namen.
2229	NERR_ACFFileIOFail	Es ist ein Platten-E/A-Fehler aufgetreten.
2230	NERR_ACFTooManyLists	Die Begrenzung von 64 Einträgen pro Ressource wurde überschritten.
2231	NERR_UserLogon	Das Löschen eines Benutzers mit einer Sitzung ist nicht zulässig.
2232	NERR_ACFNoParent	Das übergeordnete Verzeichnis wurde nicht gefunden.
2233	NERR_CanNotGrowSegment	Ein Segment des UAS-Sitzungscache konnte nicht vergrößert werden.

Fehler	Definition	Anmerkungen
2234	NERR_SpeGroupOp	Die angegebene Operation ist für diese spezielle Gruppe nicht zulässig.
2235	NERR_NotInCache	Der angegebene Benutzer wird nicht im UAS-Sitzungscache zwischengespeichert.
2236	NERR_UserInGroup	Der Benutzer gehört bereits zu der angegebenen Gruppe.
2237	NERR_UserNotInGroup	Der Benutzer gehört nicht zu der angegebenen Gruppe.
2238	NERR_AccountUndefined	Das angegebene Benutzerkonto wurde nicht definiert.
2239	NERR_AccountExpired	Das angegebene Benutzerkonto ist abgelaufen.
2240	NERR_InvalidRequester	Der Benutzer ist nicht dazu berechtigt, sich von der angegebenen Workstation aus anzumelden.
2241	NERR_InvalidLogonHours	Der Benutzer ist momentan nicht dazu berechtigt, sich anzumelden.
2242	NERR_PasswordExpired	Das Kennwort des angegebenen Benutzers ist abgelaufen.
2243	NERR_PasswordCantChange	Das Kennwort des angegebenen Benutzers kann nicht geändert werden.
2244	NERR_PasswordHistConflict	Das angegebene Kennwort kann derzeit nicht verwendet werden.
2245	NERR_PasswordTooShort	Das Kennwort ist zu kurz.
2246	NERR_PasswordTooRecent	Das Kennwort dieses Benutzers ist zu neu, um geändert werden zu können.
2247	NERR_InvalidDatabase	Die UAS-Datenbankdatei ist beschädigt.
2248	NERR_DatabaseUpToDate	Diese Kopie der UAS-Datenbank muss nicht aktualisiert werden.
2249	NERR_SyncRequired	Diese replizierende Datenbank ist bereits nicht mehr aktuell; eine Synchronisation ist erforderlich
2250	NERR_UseNotFound	Die Verbindung wurde nicht gefunden.
2251	NERR_BadAsgType	Der Typ **asg_type** ist ungültig.
2252	NERR_DeviceIsShared	Die angegebene Einheit wird momentan gemeinsam benutzt.
2270	NERR_NoComputerName	Ein Computername wurde nicht konfiguriert.
2271	NERR_MsgAlreadyStarted	Die Messenger-Dienste wurden bereits gestartet.

Fehler	Definition	Anmerkungen
2272	NERR_MsgInitFailed	Die Messenger-Dienste konnten nicht gestartet werden.
2273	NERR_NameNotFound	Der Nachrichtenaliasname konnte im lokalen Netzwerk nicht gefunden werden.
2274	NERR_AlreadyForwarded	Der angegebene Nachrichtenaliasname wurde bereits weitergeleitet.
2276	NERR_AlreadyExists	Der angegebene Nachrichtenaliasname ist bereits im lokalen System vorhanden.
2277	NERR_TooManyNames	Die maximale Anzahl an hinzugefügten Nachrichtenaliasnamen wurde überschritten.
2278	NERR_DelComputerName	Der Computername kann nicht gelöscht werden.
2279	NERR_LocalForward	Nachrichten können nicht an dieselbe Workstation zurückgeschickt werden.
2280	NERR_GrpMsgProcessor	Fehler im Nachrichtenprozessor der Domäne.
2281	NERR_PausedRemote	Die Nachricht wurde weitergeleitet, jedoch hat der Empfänger die Messenger-Dienste angehalten.
2282	NERR_BadReceive	Die Nachricht wurde zwar gesendet, jedoch nicht empfangen.
2283	NERR_NameInUse	Der Nachrichtenaliasname wird bereits verwendet. Wiederholen Sie den Vorgang später noch einmal.
2284	NERR_MsgNotStarted	Die Messenger-Dienste wurden nicht gestartet.
2285	NERR_NotLocalName	Der Name wurde nicht auf dem lokalen Computer gefunden.
2286	NERR_NoForwardName	Der Aliasname für die weitergeleitete Nachricht konnte im Netzwerk nicht gefunden werden.
2287	NERR_RemoteFull	Die Tabelle mit den Nachrichtenaliasnamen auf der fernen Datenstation ist voll.
2288	NERR_NameNotForwarded	Nachrichten für diesen Aliasnamen werden derzeit nicht weitergeleitet.
2289	NERR_TruncatedBroadcast	Die Broadcast-Nachricht wurde abgeschnitten.
2294	NERR_InvalidDevice	Hierbei handelt es sich um einen ungültigen Einheitennamen.
2295	NERR_WriteFault	Beim Schreiben ist ein Fehler aufgetreten.

Fehler	Definition	Anmerkungen
2297	NERR_DuplicateName	Auf dem lokalen Netzwerk ist ein identischer Nachrichtenaliasname vorhanden.
2298	NERR_DeleteLater	Der Nachrichtenaliasname wird zu einem späteren Zeitpunkt gelöscht.
2299	NERR_IncompleteDel	Der Nachrichtenaliasname konnte nicht in allen Netzwerken gelöscht werden.
2300	NERR_MultipleNets	Diese Operation wird nicht auf Systemen mit mehreren Netzwerken unterstützt.
2301	NERR_DASDNotInstalled	DASDN wurde nicht installiert.
2302	NERR_DASDAlreadyInstalled	DASDN wurde bereits installiert.
2303	NERR_NotHPFSVolume	—
2304	NERR_DASDMaxValidationFailed	—
2305	NERR_DASDInstallVolumeLocked	—
2306	NERR_LimitNotFound	—
2307	NERR_LimitExists	—
2308	NERR_DASDNotRunning	—
2309	NERR_DASDNotOperational	—
2310	NERR_NetNameNotFound	Die angegebene gemeinsam benutzte Ressource ist nicht vorhanden.
2311	NERR_DeviceNotShared	Die angegebene Einheit wird nicht gemeinsam benutzt.
2312	NERR_ClientNameNotFound	Es ist keine Sitzung für den angegebenen Computernamen vorhanden.
2314	NERR_FileIdNotFound	Es ist keine offene Datei mit der angegebenen ID-Nummer vorhanden.
2315	NERR_ExecFailure	Beim Ausführen eines Fernverwaltungsbefehls ist ein Fehler aufgetreten.
2316	NERR_TmpFile	Beim Öffnen einer fernen temporären Datei ist ein Fehler aufgetreten.
2317	NERR_TooMuchData	Die Daten, die von einem fernen Verwaltungsbefehl zurückgegeben wurden, wurden auf 64 KB gekürzt.
2318	NERR_DeviceShareConflict	Diese Einheit kann nicht gleichzeitig als gespoolte und nicht-gespoolte Ressource verwendet werden.
2319	NERR_BrowserTableIncomplete	Die Daten in der Serverliste sind möglicherweise nicht korrekt.
2320	NERR_NotLocalDomain	Der Computer ist in der angegebenen Domäne nicht aktiv.
2321	NERR_RedirectionsNotFound	—

Fehler	Definition	Anmerkungen
2322	NERR_LocalPathWarning	—
2323	NERR_AssignmentNotMade	—
2324	NERR_ItemNotAssigned	—
2325	NERR_CantAddAssignments	—
2326	NERR_CantSetAssignments	—
2327	NERR_DomainSpecificInfo	—
2328	NERR_TooManyLogonAsn	—
2329	NERR_DASDNoAPARs	—
2331	NERR_DevInvalidOpCode	Die Operation ist für diese Einheit ungültig.
2332	NERR_DevNotFound	Die angegebene Einheit kann nicht gemeinsam benutzt werden.
2333	NERR_DevNotOpen	Die angegebene Einheit war nicht betriebsbereit.
2334	NERR_BadQueueDevString	Die angegebene Liste mit Einheitennamen ist ungültig.
2335	NERR_BadQueuePriority	Die Warteschlangenpriorität ist ungültig.
2337	NERR_NoCommDevs	Es sind keine gemeinsamen Übertragungseinheiten vorhanden.
2338	NERR_QueueNotFound	Die angegebene Warteschlange ist nicht vorhanden.
2340	NERR_BadDevString	Die angegebene Liste mit Einheiten ist ungültig.
2341	NERR_BadDev	Die angeforderte Einheit ist ungültig.
2342	NERR_InUseBySpooler	Die angegebene Einheit wird bereits vom Spooler benutzt.
2343	NERR_CommDevInUse	Die angegebene Einheit wird bereits als DFV-Einheit verwendet.
2351	NERR_InvalidComputer	Der angegebene Computername ist ungültig.
2354	NERR_MaxLenExceeded	Die angegebene Zeichenfolge und das Präfix sind zu lang.
2356	NERR_BadComponent	Die angegebene Pfadkomponente ist ungültig.
2357	NERR_CantType	Der Typ der Eingabe kann nicht festgestellt werden.
2362	NERR_TooManyEntries	Der Typenpuffer ist nicht groß genug.
2377	NERR_LogOverflow	Die angegebene Protokolldatei überschreitet die definierte maximale Größe.

Fehler	Definition	Anmerkungen
2378	NERR_LogFileChanged	Die angegebene Protokolldatei wurde zwischen den Lesevorgängen geändert.
2379	NERR_LogFileCorrupt	Die angegebene Protokolldatei ist beschädigt.
2380	NERR_SourceIsDir	Der Quellenpfad kann kein Verzeichnis sein.
2381	NERR_BadSource	Der Quellenpfad ist ungültig.
2382	NERR_BadDest	Der Zielpfad ist ungültig.
2383	NERR_DifferentServers	Der Quellen- und der Zielpfad befinden sich auf unterschiedlichen Servern.
2385	NERR_RunSrvPaused	Der angeforderte Server wurde angehalten.
2389	NERR_ErrCommRunSrv	Bei der Kommunikation mit einem Server ist ein Fehler aufgetreten.
2391	NERR_ErrorExecingGhost	Beim Starten eines Hintergrundprozesses ist ein Fehler aufgetreten.
2392	NERR_ShareNotFound	Die gemeinsam benutzte Ressource, mit der Sie verbunden sind, konnte nicht gefunden werden.
2400	NERR_InvalidLana	Die LAN-Adapternummer ist ungültig.
2401	NERR_OpenFiles	In der Verbindung sind offene Dateien vorhanden.
2402	NERR_ActiveConns	Es sind immer noch aktive Verbindungen vorhanden.
2403	NERR_BadPasswordCore	Der angegebene Netzwerkname bzw. das Kennwort ist ungültig.
2404	NERR_DevInUse	Ein aktiver Prozess greift momentan auf die Einheit zu.
2405	NERR_LocalDrive	Der Laufwerkbuchstabe wird lokal verwendet.
2406	NERR_PausedConns	Angehaltene Einheiten können nicht gelöscht werden.
2407	NERR_PipeBufTooSmall	Schreibt an ein Netzwerk mit einem benannten Pipe-Puffer, dem zu wenig Speicherplatz zugeordnet ist.
2430	NERR_AlertExists	Der angegebene Client ist bereits für das angegebene Ereignis registriert.
2431	NERR_TooManyAlerts	Die Alert-Tabelle ist voll.
2432	NERR_NoSuchAlert	Es wurde ein ungültiger oder nicht vorhandener Alert-Name angegeben.
2433	NERR_BadRecipient	Der Alert-Empfänger ist ungültig.

Fehler	Definition	Anmerkungen
2434	NERR_AcctLimitExceeded	Eine Benutzersitzung für diesen Server wurde gelöscht.
2440	NERR_InvalidLogSeek	Die Protokolldatei enthält nicht die angeforderte Datensatznummer.
2450	NERR_BadUasConfig	Die Systemdatenbank für Benutzerkonten wurde nicht ordnungsgemäß konfiguriert.
2451	NERR_InvalidUASOp	Diese Operation ist während der Ausführung des Netlogon-Dienstes nicht zulässig.
2452	NERR_LastAdmin	Die angegebene Operation ist für das letzte Administratorenkonto nicht zulässig.
2453	NERR_DCNotFound	Der Domänencontroller für diese Domäne konnte nicht gefunden werden.
2454	NERR_LogonTrackingError	Die Anmeldedaten für diesen Benutzer konnten nicht gesetzt werden.
2455	NERR_NetlogonNotStarted	Der Netlogon-Dienst wurde nicht gestartet.
2456	NERR_CanNotGrowUASFile	Die Systemdatenbank für Benutzerkonten konnte nicht vergrößert werden.
2458	NERR_PasswordMismatch	Es wurde eine Kennwortabweichung festgestellt.
2459	NERR_MaxBadPasswordExceeded	Die Nummer des ungültigen Kennworts.
2460	NERR_NoSuchServer	Die Server-ID gibt keinen gültigen Server an.
2461	NERR_NoSuchSession	Die Sitzungs-ID gibt keine gültige Sitzung an.
2462	NERR_NoSuchConnection	Die Verbindungs-ID gibt keine gültige Verbindung an.
2463	NERR_TooManyServers	Der Platz reicht nicht aus, um der Liste mit den verfügbaren Servern einen weiteren Eintrag hinzuzufügen.
2464	NERR_TooManySessions	Der Server hat die maximale Anzahl der unterstützten Sitzungen erreicht.
2465	NERR_TooManyConnections	Der Server hat die maximale Anzahl der unterstützten Verbindungen erreicht.
2466	NERR_TooManyFiles	Der Server kann keine weiteren Dateien öffnen, da die maximale Anzahl erreicht wurde.

Fehler	Definition	Anmerkungen
2467	NERR_NoAlternateServers	Auf diesem Server sind keine alternativen Server registriert.
2480	NERR_UPSDriverNotStarted	Der UPS-Dienst konnte auf den UPS-Treiber nicht zugreifen.
2500	NERR_BadDosRetCode	Das folgende Programm hat einen MS-DOS-Fehlercode zurückgegeben.
2501	NERR_ProgNeedsExtraMem	Das folgende Programm benötigt mehr Speicherplatz.
2502	NERR_BadDosFunction	Das folgende Programm hat eine MS-DOS-Funktion aufgerufen, die nicht unterstützt wird:
2503	NERR_RemoteBootFailed	Die Workstation konnte nicht gebootet werden.
2504	NERR_BadFileCheckSum	Die folgende Datei ist beschädigt.
2508	NERR_ImageParamErr	Parametersubstitution für Image ist fehlgeschlagen.
2509	NERR_TooManyImageParams	Die Anzahl der Imageparameter, die Plattensektorgrenzen überschreiten, ist zu hoch.
2510	NERR_NonDosFloppyUsed	Das Image wurde nicht von einer MS-DOS-Diskette, die mit /S formatiert wurde, generiert.
2513	NERR_CantConnectRplSrvr	Es kann keine Verbindung zum **Remoteboot**-Server hergestellt werden.
2514	NERR_CantOpenImageFile	Imagedatei auf dem **Remoteboot**-Server konnte nicht geöffnet werden.
2515	NERR_CallingRplSrvr	Verbindung zum **Remoteboot**-Server wird hergestellt.
2516	NERR_StartingRplBoot	Verbindung zum **Remoteboot**-Server wird hergestellt.
2525	NERR_FTNotInstalled	**DISKFT.SYS** ist nicht installiert worden.
2526	NERR_FTMONITNotRunning	**FTMONIT** ist nicht aktiv.
2527	NERR_FTDiskNotLocked	Der Prozess **FTADMIN** hat den Datenträger nicht gesperrt.
2528	NERR_FTDiskNotAvailable	Ein anderer Prozess hat den Datenträger gesperrt.
2529	NERR_FTUnableToStart	Das Prüf- bzw. Korrekturprogramm kann nicht gestartet werden.
2530	NERR_FTNotInProgress	Das Prüf- bzw. Korrekturprogramm kann nicht abgebrochen werden, da es nicht gestartet wurde.

Fehler	Definition	Anmerkungen
2531	NERR_FTUnableToAbort	Das Prüf- bzw. Korrekturprogramm kann nicht abgebrochen werden.
2532	NERR_FTUnabletoChange	Der Datenträger konnte nicht ge- bzw. entsperrt werden.
2533	NERR_FTInvalidErrHandle	Die Fehlerbehandlung wurde nicht erkannt.
2534	NERR_FTDriveNotMirrored	Das Laufwerk wird nicht gespiegelt.
2781	NERR_NoAccessDrive	—
2782	NERR_AliasExists	—
2783	NERR_AliasNotFound	—
2785	NERR_InvAliasDev	—
2786	NERR_DCDBError	—
2787	NERR_NetnameExists	—
2788	NERR_DupAliasRes	—
2792	NERR_AppExists	—
2793	NERR_AppNotFound	—
2794	NERR_DCDBCreateError	—
2795	NERR_NotPrimaryDCDB	—
2796	NERR_BadAppRemark	—
2800	NERR_ApplyNotPermitted	—
2801	NERR_IncompleteApply	—
2802	NERR_ApplyFailed	—

OS/2-Verteilungsfehler

In diesem Abschnitt werden die Nachrichten aufgelistet und erläutert, die beim Auftreten von Verteilungsfehlern von Tivoli User Administration for OS/2 ausgegeben werden.

FEHLER 101

Erläuterung: Während der Profilverteilung ist ein allgemeiner Fehler aufgetreten. Mit Hilfe des angezeigten Net32 API-Ergebniscodes können Sie möglicherweise die Ursache des Verteilungsfehlers feststellen.

Bedieneraktion: Nicht zutreffend

FEHLER 102:

Erläuterung: Das Benutzerprofil, das an den OS/2-Endpunkt verteilt wurde, enthält keine OS/2-spezifischen Daten.

Bedieneraktion: Nicht zutreffend

FEHLER 103

Erläuterung: Der Tivoli-Verwaltungsagent, der unter OS/2 ausgeführt wird, hat eine Fehlernachricht erhalten. Die OS/2-Fehlernummer wird angezeigt. Mögliche Ursachen hierfür sind:

- Der Tivoli-Verwaltungsagent hat auf einen ungültigen Speicher zugegriffen.
- Der Tivoli-Verwaltungsagenten-Prozess wurde gestoppt.
- Die Speicherkapazität des Tivoli-Verwaltungsagenten ist erschöpft.

Bedieneraktion: In der Include-Datei bsexcpt.h des OS/2-Toolkits C finden Sie die Definitionen der OS/2-Fehler.

FEHLER 104

Erläuterung: Der Tivoli-Verwaltungsagent auf dem OS/2-Endpunkt konnte keine Verbindung mit dem TMR-Server herstellen.

Bedieneraktion: Nicht zutreffend

FEHLER 105

Erläuterung: Der Tivoli-Verwaltungsagent wird auf einem primären (oder Back-up-) OS/2-Domänencontroller ausgeführt, und an diesem System wurden keine Konten mit Administratorberechtigungen angemeldet. Ein Konto mit Administratorberechtigungen ist für die Verwaltung des Basisverzeichnisses erforderlich.

Bedieneraktion: Erstellen Sie ein Konto mit Administratorberechtigungen für die Verwaltung des Basisverzeichnisses.

FEHLER 203

Erläuterung: Während eines Weitergabevorgangs hat der Tivoli-Verwaltungsagent einen OS/2-Fehler empfangen.

Bedieneraktion: Die Fehlernummer wird angezeigt. Siehe FEHLER 103.

FEHLER 205

Erläuterung: Der Tivoli-Verwaltungsagent kann den Weitergabevorgang nicht ausführen, da kein Konto mit Administratorberechtigungen angemeldet wurde.

Bedieneraktion: Nicht zutreffend

FEHLER 206

Erläuterung: Der Tivoli-Verwaltungsagent kann den Weitergabevorgang nicht ausführen, da die Net32-APIs einen Fehlercode zurückgegeben haben.

Bedieneraktion: Der Ergebniscode wird angezeigt. Siehe Anhang A in diesem Handbuch.

FEHLER 301

Erläuterung: Der Tivoli-Verwaltungsagent kann das Kennwort nicht ändern, da die Net32-APIs einen Fehlercode zurückgegeben haben.

Bedieneraktion: Der Ergebniscode wird angezeigt. Siehe Anhang A in diesem Handbuch.

FEHLER 302

Erläuterung: Der Tivoli-Verwaltungsagent kann das Kennwort nicht ändern, da der Benutzer auf dem angegebenen Endpunkt unbekannt ist.

Bedieneraktion: Nicht zutreffend

FEHLER 303

Erläuterung: Der Tivoli-Verwaltungsagent kann das Kennwort nicht ändern, da die Entschlüsselung fehlgeschlagen ist.

Bedieneraktion: Nicht zutreffend

FEHLER 304

Erläuterung: Der Tivoli-Verwaltungsagent kann den Weitergabevorgang nicht ausführen, da die Net32-APIs einen Fehlercode zurückgegeben haben. Der Tivoli-Verwaltungsagent kann das Kennwort nicht ändern, da kein Konto mit Administratorberechtigungen angemeldet wurde.

Bedieneraktion: Erstellen Sie, falls notwendig, ein Konto mit Administratorberechtigungen, und melden Sie sich an.

Glossar

Dieses Glossar enthält die in Zusammenhang mit dem Tivoli-Produkt verwendete Terminologie sowie ausgewählte Begriffe und Definitionen, die folgendem Buch entnommen sind:

- Dem vom American National Standards Institute herausgegebenen Wörterbuch 'American National Standard Dictionary for Information Systems', ANSI X3.172-1990 (Copyright 1990). Sie können dieses Wörterbuch beim American National Standards Institute, 11 West 42nd Street, New York, New York 10036, bestellen. Definitionen aus diesem Wörterbuch sind mit (A) gekennzeichnet.
- Information Technology Vocabulary, erstellt von Subcommittee 1, Joint Technical Committee 1 der International Organization for Standardization und der International Electrotechnical Commission (ISO/IEC JTC1/SC1). Die Definitionen aus diesem Wörterbuch sind durch das Symbol (I) nach der jeweiligen Definition gekennzeichnet. Das Symbol (T) nach einer Definition kennzeichnet Entwürfe für internationale Standards und Arbeitspapiere der Komitees, die derzeit von ISO/IEC und JTC1/SC1 erstellt werden, jedoch von den beteiligten nationalen Körperschaften von SC1 noch nicht abgesegnet worden sind.
- IBM Dictionary of Computing, New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, Glossary of Networking Terms
- Internet Request for Comments: 1392, Internet Users' Glossary
- The Object-Oriented Interface Design: IBM Common User Access Guidelines, Carmel, Indiana: Que, 1992.

A

Abwärts gerichteter Aufruf
In einer Tivoli-Umgebung ein „abwärts" an einen Endpunkt gerichteter Methodenaufruf eines TMR-Servers oder -Gateways. *Gegensatz zu* Aufwärts gerichteter Aufruf.

ADE

Siehe Tivoli Application Development Environment.

AEF

*Siehe*Tivoli Application Extension Facility .

Aufwärts gerichteter Aufruf

In einer Tivoli-Umgebung ein „aufwärts" an ein Gateway gerichteter Methodenaufruf eines Endpunkts. *Gegensatz zu* Abwärts gerichteter Aufruf.

Ausgabefächerung

Bei der Datenübertragung das Erstellen von Kopien einer Verteilung, die lokal oder über ein Netzwerk gesendet werden.

B

Berechtigungsklasse

In einer Tivoli-Umgebung wird Tivoli-Administratoren eine Berechtigungsklasse zugewiesen, die ihnen die Ausführung der ihnen zugewiesenen Systemverwaltungs-Tasks ermöglicht. Eine Berechtigungsklasse kann für die gesamte Tivoli Management Region (TMR) oder für bestimmte Ressourcen, wie z. B. die, die in einem Richtlinienbereich enthalten sind, erteilt werden. Beispiele für Berechtigungsklassen sind: super, senior, admin, user u. a.

D

Dämon

Ein Programm, das einen Standarddienst im nicht überwachten Modus ausführt. Einige Dämonen werden automatisch ausgelöst, andere führen in regelmäßigen Abständen ihre Tasks aus.

Datenbankmodus des Profilmanagers

Siehe Profilmanager.

Datenloser Modus des Profilmanagers

Siehe Profilmanager.

E

Endpunkt

In einer Tivoli-Umgebung ein Tivoli-Client, der letztendlich der Empfänger einer Tivoli-Operation ist.

In einer Tivoli-Umgebung ein Tivoli-Dienst, der auf mehreren Betriebssystemen aktiv ist und auf diesen Systemen Tivoli-Operationen ausführt, die es Tivoli Management Framework ermöglichen, diese Systeme als Tivoli-Clients zu verwalten.

Endpunktliste
Eine Liste mit allen Endpunkten in der TMR und die zugeordneten Gateways. Diese Liste wird vom Endpunktmanager verwaltet. *Siehe auch* Endpunktmanager.

Endpunktmanager
In einer Tivoli-Umgebung ein Dienst, der auf dem Tivoli-Server aktiv ist, Gateways und Endpunkte steuert und konfiguriert, Endpunkte und Gateways einander zuordnet und die Endpunktliste verwaltet.

Endpunktmethode
In einer Tivoli-Umgebung eine Methode, die als Ergebnis einer Anforderung von anderen verwalteten Ressourcen in der Tivoli Management Region auf einem Endpunktclient ausgeführt wird. Die Ergebnisse der Methode werden zuerst an das Gateway und anschließend an die aufrufende verwaltete Ressource weitergeleitet.

Ereignis
In einer Tivoli-Umgebung alle bedeutenden Änderungen am Status einer Systemressource oder einer Anwendung. Auch ein Ereignisbericht wird ebenfalls als Ereignis bezeichnet. Ein Ereignis kann für ein Problem sowie für die erfolgreiche Fertigstellung einer Task generiert werden. Beispiele für Ereignisse sind: der normale Vorgang zum Starten und Stoppen eines Prozesses und die fehlerhafte Funktionsweise eines Servers.

Ereignis-Repository
In einer Tivoli-Umgebung ein RIM-Repository, das Informationen enthält, die von Tivoli Enterprise Console gesammelt oder generiert werden. Zum Beispiel speichert Tivoli Enterprise Console im Ereignis-Repository Informationen zu Ereignissen.

F

Ferne Verteilung
In einer Tivoli-Umgebung eine Verteilung an Zielmaschinen, die sich in einer verbundenen Tivoli Management Region (TMR) befinden.

G

Gateway
Eine Funktionseinheit, die zwei Computernetzwerke mit unterschiedlichen Netzwerkarchitekturen miteinander verbindet. Ein Gateway verbindet Netzwerke oder Systeme mit unterschiedlichen Architekturen. Eine Brücke (Bridge) verbindet Netzwerke oder Systeme mit denselben oder verwandten Architekturen.
Eine Funktionseinheit, die zwei Netzwerke oder Teilnetzwerke mit unterschiedlichen Kenndaten verbindet, z. B. mit unterschiedlichen Protokollen oder unterschiedlichen Richtlinien zur Sicherheit oder Übertragungspriorität.
Die Kombination von Maschinen und Programmen, die Adressumsetzung, Namensumsetzung und SSCP-Rufweiterschaltung (SSCP, System Services Control Point)

zwischen unabhängigen SNA-Netzwerken zur Verfügung stellen, die diesen Netzwerken die Kommunikation untereinander ermöglicht. Ein Gateway besteht aus einem Gateway-NCP (Network Control Programm) und mindestens einem Gateway-VTAM.
In einer Tivoli-Umgebung eine Software auf einem verwalteten Knoten, die alle Übertragungsdienste zwischen einer Gruppe von Endpunkten und der übrigen Tivoli-Umgebung herstellt. Das Gateway verfügt über die MDist-Funktion (Multiplexed Distribution) und kann so als Ausgabefächerungspunkt Verteilungen an eine Vielzahl von Endpunkten vornehmen.

H

Hinweis

In einer Tivoli-Umgebung eine von einer Systemverwaltungsoperation generierte Nachricht, die Informationen zu einem Ereignis oder dem Status einer Anwendung enthält. Die Hinweise werden in Hinweisgruppen gespeichert. *Siehe auch* Schwarzes Brett.

Hinweisgruppe

In einer Tivoli-Umgebung ein anwendungs- oder vorgangsspezifischer Container, der auf bestimmte Tivoli-Funktionen bezogene Hinweise speichert und anzeigt. Das Schwarze Brett von Tivoli besteht aus Hinweisgruppen. Einem Tivoli-Administrator können eine oder mehrere Hinweisgruppe(n) zugeordnet werden; das Schwarze Brett des Administrators enthält nur die Hinweise aus einer Hinweisgruppe, die dem Administrator zugeordnet wurden.

I

Installations-Repository (IR)

In Tivoli Software Installation Service (SIS) das Verzeichnis mit wiederverwendbaren Installationsimages und weiteren Daten, die von SIS verwendet werden.

Instanz

In der objektorientierten Programmierung ein Objekt, das auf Basis eines für eine Klasse vorgegebenen Instanzmodells erstellt wurde.

J

Job

Eine von einem Benutzer definierte Arbeitseinheit, die von einem Computer ausgeführt wird. Manchmal wird mit diesem Begriff auch lediglich eine Darstellung eines Jobs bezeichnet. Diese Darstellung kann eine Reihe von Computerprogrammen, Dateien und Steueranweisungen für das Betriebssystem enthalten.

In einer Tivoli-Umgebung eine Ressource, die aus einer Task und deren vorkonfigurierten Ausführungsparametern besteht. Die Ausführungsparameter legen unter anderem die Gruppe der Hosts fest, auf denen der Job ausgeführt werden soll.

K

Kanonisch
In der Computerwissenschaft ein Ausdruck, der einer bestimmten Menge von Regeln entspricht.

Klasse
1) In der objektorientierten Entwicklung oder Programmierung eine Gruppe von Objekten mit einer gemeinsamen Definition, d. h. mit gemeinsamen Merkmalen, Operationen und Verhaltensweisen. Die Mitglieder der Gruppe werden Klasseninstanzen genannt. 2) Im Betriebssystem AIX bezieht sich 'Klasse' auf die E/A-Eigenschaften einer Einheit. Systemeinheiten werden als Block- oder Zeicheneinheiten klassifiziert.

Klonen
In einer Tivoli-Umgebung eine Operation, mit der ein Tivoli-Administrator Profile replizieren kann. Diese Fähigkeit erleichtert die Erstellung mehrerer Profile mit verwandten Merkmalen. *Siehe auch* Profilprototyp.

Konfigurationsprogramm
In Tivoli Software Distribution eine Funktion, mit der ein Tivoli-Administrator Operationen (a) vor oder nach der Verteilung eines Dateipakets, (b) vor oder nach der Entfernung eines Dateipakets, (c) während der Festschreibung eines Dateipakets oder (d) nach Abbruch einer Verteilung oder Entfernung aufgrund eines Fehlers durchführen können.

Konfigurations-Repository
Die relationale Datenbank, die Informationen enthält, die von Tivoli-Anwendungen gesammelt oder generiert werden. Zum Beispiel speichert Tivoli Inventory im Konfigurations-Repository Informationen zur Hardware, Software, Systemkonfiguration und zum Inventar. Tivoli Software Distribution speichert Informationen zu Dateipaketoperationen. Tivoli Enterprise Console speichert Informationen zu Ereignissen.

L

Lokale Änderungen
In einer Tivoli-Umgebung eine Funktion aller Tivoli-Anwendungen, die auf der Grundlage von Profilen arbeiten (Tivoli Software Distribution stellt jedoch eine Ausnahme dar). Diese Funktion ermöglicht es, die Änderungen in einem verteilten Profil durch die Änderungen, die in einem Endpunktprofil vorgenommen wurden, zu überschreiben.

Lokale Verteilung
In einer Tivoli-Umgebung eine Verteilung an Zielmaschinen, die sich in derselben Tivoli Management Region (TMR) wie die Quellenmaschine befinden.

M

MDist
Multiplexverteilung. In einer Tivoli-Umgebung ein Dienst, der die effiziente Verteilung großer Datenmengen in komplexen Netzwerken ermöglicht. Bei MDist 1 und MDist 2 handelt es sich um zwei Varianten der Multiplexverteilungstechnologie. MDist 2 ist dabei eine Erweiterung von MDist 1, die in der Lage ist, die anspruchsvollen Verteilungsanforderungen der Softwareanwendungen von Tivoli Enterprise zu erfüllen.

N

Namensregistrierdatenbank
In einer Tivoli-Umgebung ein Namensdienst, der aus einer zweidimensionalen Tabelle besteht, mit deren Hilfe in einer Tivoli Management Region (TMR) Ressourcennamen zu Ressourcen-IDs und zugehörigen Informationen zugeordnet werden.

NetWare-verwaltete Station
In einer Tivoli-Umgebung eine Ressource, die (a) einen Novell NetWare-Server, auf dem Tivoli NetWare Repeater (TNWR) installiert ist, und (b) einen oder mehrere Client(s) darstellt. Eine NetWare-verwaltete Station ermöglicht die Verteilung von Profilen durch den NetWare-Server an mindestens einen angegebenen Client-PC über TCP/IP oder IPX.

O

Objekt
(1) In der objektorientierten Entwicklung oder Programmierung eine konkrete Realisierung einer Klasse, die aus Daten und Operationen besteht, die diesen Daten zugeordnet sind. (2) In einer objektorientierten Entwicklung oder Programmierung ein Objekt, das eine Instanz einer Klasse ist. Eine Klasse ist ein Modell oder eine Schablone. Wenn einer Klasse ein Konstruktor zugeordnet wird, wird ein Objekt erstellt mit den Merkmalen und Verhaltensweisen, die für die Klasse definiert wurden. Merkmale werden als Attributwerte angegeben. Das Verhalten ist in Methoden definiert.

Objektgruppe
In einer Tivoli-Umgebung ein Container, der Objekte auf einer Tivoli-Arbeitsoberfläche zu Gruppen zusammenfasst und so dem Tivoli-Administrator eine einzige Ansicht zusammenzugehöriger Ressourcen bietet. Objektgruppen können entweder

von Tivoli Management Framework oder einem Tivoli-Administrator erstellt werden. Die Bestandteile einer Objektgruppe werden als Mitglieder bezeichnet. Beispiele für Objektgruppen sind die Administratorobjektgruppe und die generische Objektgruppe; die Administratorobjektgruppe ist ein Beispiel für eine von Tivoli Management Framework erstellte Objektgruppe.

Objektpfad
In einer Tivoli-Umgebung ein absoluter oder relativer Pfad eines Tivoli-Objekts, ähnlich dem Pfad in einem Dateisystem.

Objektverweis
In einer Tivoli-Umgebung die Kennung (OID = Object Identifier), die einem Objekt während seiner Erstellung zugeordnet wird.

oserv
Der Name des CORBA-kompatiblen Object Request Broker (ORB), der in der Tivoli-Umgebung verwendet wird. Oserv wird auf dem TMR-Server und allen zugehörigen verwalteten Knoten ausgeführt.

P

Profil
In einer Tivoli-Umgebung ein Container für anwendungsspezifische Informationen zu einer bestimmten Ressourcenart. Eine Tivoli-Anwendung gibt die Schablone für ihre Profile an. Die Schablone enthält Informationen zu den Ressourcen, die von einer Tivoli-Anwendung verwaltet werden können.
Profile werden im Profilmanager erstellt. Der Profilmanager verbindet das Profil mit einer Tivoli-Ressource (beispielsweise einem verwalteten Knoten), die die im Profil enthaltenen Informationen verwendet. Ein Profil hat keine direkten Subskribenten.

Profilmanager
In einer Tivoli-Umgebung ein Container für Profile, der die Profile mit einer Gruppe von Ressourcen, so genannten *Subskribenten* verbindet. Tivoli-Administratoren verwalten und verteilen mit Hilfe des Profilmanagers Profile. Ein Profilmanager wird in einem Richtlinienbereich erstellt und stellt darin eine verwaltete Ressource dar. Ein Profilmanager kann in einem der folgenden beiden Modi arbeiten:

- *Datenloser Modus*: Ermöglicht dem Profilmanager, Verteilungen an alle Tivoli-Clients (verwaltete Knoten, Endpunkte, PC-verwaltete Knoten und NetWare-verwaltete Stationen), nicht jedoch an andere Profilmanager vorzunehmen.
- *Datenbankmodus*: In diesem Modus kann ein Profilmanager Verteilungen an andere Profilmanager (im datenlosen Modus oder im Datenbankmodus), an alle verwaltete Knoten, PC-verwaltete Knoten und NetWare-verwaltete Stationen, nicht jedoch an Endpunkte, vornehmen.

Profilprototyp
In einer Tivoli-Umgebung ein Profilmodell, das von Tivoli-Administratoren als Vorlage zur Erstellung anderer Profile verwendet werden kann. Oft geschieht dies durch Klonen des Profilprototyps.

Proxy-verwalteter Knoten
In einer Tivoli-Umgebung eine verwaltete Ressource, die die Kommunikation zwischen TMR-Server und einem PC, auf dem der PC-Agent aktiv ist, ermöglicht.

Pull
In einer Tivoli-Umgebung eine Operation (beispielsweise eine Tivoli UserLink Dateipaketanforderung), die eine Aktion einleitet, indem sie diese von einer Ressource anfordert. *Gegensatz zu* Push.

Push
In einer Tivoli-Umgebung eine Operation (beispielsweise eine Dateipaketverteilung), die Informationen an andere Ressourcen weitergibt. *Gegensatz zu* Pull.

R

RDBMS
Siehe Verwaltungssystem für relationale Datenbanken.

RDBMS Interface Module (RIM)
In Tivoli Management Framework das Modul in der verteilten Objektdatenbank, das Informationen zur Installation des Verwaltungssystems für relationale Datenbanken (RDBMS, Relational Database Management System) enthält.

Registrierter Name
In einer Tivoli-Umgebung der Name, unter dem eine bestimmte Ressource bei ihrer Erstellung in der Namensregistrierdatenbank registriert wird.

Repeater-Reichweite
In einer Tivoli-Umgebung die Tivoli-Clients, die Daten von der Repeater-Station empfangen.

Repeater-Station
In einer Tivoli Management Region (TMR) ein verwalteter Knoten, der mit Hilfe der MDist-Funktion konfiguriert wird. Eine Repeater-Station erhält eine Kopie der Daten und verteilt sie an die nächste Staffel von Clients.

Ressource
(1) Objekte innerhalb der Datenbank. Es gibt verwaltete Ressourcen und Ressourcen, die nicht verwaltet werden. Ressourcen, die nicht verwaltet werden, können über die Tivoli-Arbeitsoberfläche angezeigt werden. Siehe verwaltete Ressource. (2) Alle Arten von begrenzten Ressourcen wie beispielsweise Bandtreiber, Übertragungsleitungen, Datenbanken oder Drucker, die für die Ausführung eines

Jobs benötigt werden. Sie bestimmen, zu welchem Zeitpunkt und in welchem Umfang eine Ressource verfügbar ist, und welche logischen Workstations die Ressource verwenden können. Mit Hilfe dieser Informationen können Sie festlegen, zu welchem Zeitpunkt Jobnetzwerkinstanzen ausgeführt werden sollen. In der grafischen Benutzerschnittstelle (GUI) werden Ressourcen auch logische Ressourcen genannt. (3) Jede von einem Job oder einer Task benötigte Funktion eines Computersystems oder eines Betriebssystems, die über Hauptspeicher, Ein-/Ausgabeeinheiten, eine Verarbeitungseinheit, Datenbestände und Steuerungs- bzw. Verarbeitungsprogramme verfügt. *Siehe auch* Verwaltete Ressource.

Ressourcenart

In einer Tivoli-Umgebung eines der Merkmale für eine verwaltete Ressource. Ressourcenarten werden in den Standardwertegruppen eines Richtlinienbereichs definiert.

In Tivoli NetView for OS/390 eines der drei Elemente (neben dem Dateityp und der Anzeigeart), die zur Beschreibung des Aufbaus einer Anzeige verwendet werden. Ressourcenarten der einen Kategorie sind Zentraleinheit, Kanal, Controller und E/A-Einheit; in der anderen Kategorie sind es DFV-Controller, Adapter, Link, Cluster Controller und Terminal.

Richtlinie

In einer Tivoli-Umgebung eine Gruppe von auf verwaltete Ressourcen angewendete Regeln. Eine spezielle Regel in einer Richtlinie wird als „Richtlinienmethode" bezeichnet.

Richtlinienbereich

In einer Tivoli-Umgebung eine Gruppe von verwalteten Ressourcen, die mindestens eine allgemeine Richtlinie gemeinsam nutzen. Tivoli-Administratoren arbeiten mit Richtlinienbereichen, um die Verwaltung und organisatorische Struktur einer Network Computing-Umgebung festzulegen. Administratoren können ähnliche Ressourcen zu Gruppen zusammenfassen, den Zugriff auf Ressourcen definieren, Ressourcen steuern sowie Regeln zur Verwaltung der Ressourcen zuordnen. Der Richtlinienbereich umfasst Ressourcenarten und eine Liste der zu verwaltenden Ressourcen. Ein Richtlinienbereich wird auf der Tivoli-Arbeitsoberfläche durch ein Symbol dargestellt, das die Form einer Kuppel hat. Bei der Erstellung einer Tivoli Management Region (TMR) wird auch ein Richtlinienbereich mit demselben Namen erstellt. In diesem Fall verfügt die TMR nur über einen Richtlinienbereich. In den meisten Fällen erstellt der Tivoli-Administrator jedoch weitere Richtlinienbereiche und Unterbereiche, um die Struktur der TMR darzustellen. Eine TMR bezieht sich auf die tatsächliche physische Konnektivität, ein Richtlinienbereich dagegen auf die logische Anordnung der Ressourcen.

Richtlinienunterbereich

In einer Tivoli-Umgebung ein Richtlinienbereich, der sich in einem anderen Richtlinienbereich befindet oder dort erstellt wurde. Wenn ein Richtlinienunterbereich erstellt wird, verwendet er automatisch die Ressourcen- und Richtlinienmerkmale des übergeordneten Richtlinienbereichs. Der Tivoli-Administrator kann

diese Merkmale nach der Erstellung ändern oder anpassen, so dass sie den spezifischen Erfordernissen und Besonderheiten des Unterbereichs entsprechen.

Richtlinie für Gültigkeitsprüfung
In einer Tivoli-Umgebung eine Richtlinie, die sicherstellt, dass alle Ressourcen in einem Richtlinienbereich mit den für den Bereich festgelegten Richtlinien übereinstimmen. Die Richtlinie für Gültigkeitsprüfung verhindert, dass Tivoli-Administratoren Ressourcen erstellen oder ändern, die den Richtlinien des Richtlinienbereichs, in dem die Ressourcen erstellt wurden, nicht entsprechen.

Root-Administrator
In einer Tivoli-Umgebung das Konto für den ersten Tivoli-Administrator, das während der Installation von Tivoli Management Framework eingerichtet wird.

S

Schwarzes Brett
In der Tivoli-Umgebung der primäre Mechanismus, über den Tivoli Management Framework und Tivoli-Anwendungen mit den Tivoli-Administratoren kommunizieren. Das Schwarze Brett ist ein Symbol auf der Tivoli-Arbeitsoberfläche, über das Administratoren auf Hinweise zugreifen können. Tivoli-Anwendungen verwenden das Schwarze Brett als Prüfprotokoll für wichtige Vorgänge, die von den Administratoren ausgeführt werden.

Sicherheitsgruppe
In einer Tivoli-Umgebung eine Gruppe von verwalteten Ressourcen, für die ein Tivoli-Administrator Berechtigungen hat. Beispiele für Sicherheitsgruppen sind u.a. Richtlinienbereiche und die Administratorobjektgruppe.

Sicherheitsprofil
In Tivoli SecureWay Security Manager ein Profil, das Daten zur Sicherheitsverwaltung enthält. Jeder Datensatz des Sicherheitsprofils wird in einem systemunabhängigen Format gespeichert, so dass die Profildatensätze auch in einem Unternehmen verteilt werden können, das über verschiedene Systemtypen verfügt.

Sicherheitsstufen
Sicherheitsstufen bzw. Sicherheitsberechtigungen steuern den Zugriff von Benutzern und Gruppen auf bestimmte Systemaktionen.

Sicherheitsverwaltung
(1) Eine der vier grundlegenden Verwaltungsaufgaben, die mit der Tivoli-Produktlinie wahrgenommen werden können. Bei dieser Aufgabe handelt es sich um die Zugriffssteuerung für Anwendungen und Daten, die innerhalb eines Unternehmens von entscheidender Bedeutung sind. *Siehe* Verfügbarkeitsverwaltung, Einsatzverwaltung und Betrieb und Administration. (2) Eine Komponente, die mit GSO verwendet werden kann, um GSO-Sicherheitsressourcen zu verwalten. Die

Sicherheitsverwaltung ermöglicht das Erstellen und Verwalten von GSO-Benutzeranmeldungen, das Erstellen und Verwalten der GSO-Zielkennwortrichtlinie und das Ändern der Kennwortrichtlinie.

Skalierbar
Bezieht sich auf die Fähigkeit eines Systems, sich schnell an eine Steigerung oder Verringerung der Auslastung, des Datenbestands oder der Anforderungen anzupassen. Ein skalierbares System kann sich beispielsweise effizient an die Arbeit mit größeren oder kleineren Netzwerken zur Ausführung von Tasks unterschiedlicher Komplexität anpassen.

Subskribent
In einer Tivoli-Umgebung ein verwalteter Knoten, ein Profilmanager, ein Endpunkt oder ein anderer Tivoli-Client, der einem Profilmanager als Teilnehmer zugeordnet ist. Obwohl Profile an Subskribenten verteilt werden, sind die Subskribenten nicht immer der endgültige Zielort der verteilten Profile.

Standardwertegruppe
In einer Tivoli-Umgebung eine Gruppe von Merkmalwerten, die einer Ressource bei ihrer Erstellung zugeordnet werden.

Subskription
In einer Tivoli-Umgebung der Prozess zur Identifikation der verwalteten Ressourcen, an die Profile verteilt werden. Verwaltete Ressourcen und Profile werden über Profilmanager einander zugeordnet.

Subskriptionsliste
In der Tivoli-Umgebung eine Liste mit den verwalteten Ressourcen, die einem Profilmanager als Subskribenten zugeordnet sind. Diese verwalteten Ressourcen (die andere Profilmanger enthalten können) sind die Empfänger der Profilverteilungen. Durch die Angabe eines Profilmanagers in einer Subskriptionsliste (also durch Angabe einer Liste in einer Liste) können mehrere verwaltete Ressourcen gleichzeitig als Subskribenten zugeordnet werden, anstatt sie nacheinander zuzuordnen.

T

Task
(1) In einer Tivoli-Umgebung die Definition einer Aktion, die routinemäßig auf verschiedenen Tivoli-Clients im gesamten Netzwerk ausgeführt werden muss. Eine Task definiert die für die Task erforderlichen ausführbaren Dateien, die für die Ausführung der Task erforderliche Berechtigungsklasse sowie den Namen des Benutzers oder der Gruppe, unter dem die Task ausgeführt wird. (2) In GSO die Definition einer Aktion, die routinemäßig auf verschiedenen verwalteten Knoten im gesamten Netzwerk ausgeführt werden muss. Eine Task definiert die für die Task erforderli-

chen ausführbaren Dateien, die für die Ausführung der Task erforderliche Berechtigungsklasse sowie den Namen des Benutzers oder der Gruppe, unter dem die Task ausgeführt wird.

Task-spezifische Berechtigungsklasse
In Tivoli SecureWay Security Manager und Tivoli SecureWay User Administration eine Berechtigungsklasse, die die Ausführung genau definierter verwaltungsspezifischer Aufgaben vornehmen.

Tivoli-Administrator
In einer Tivoli-Umgebung ein Systemadministrator, der zum Ausführen von Systemverwaltungs-Tasks und Verwalten von Richtlinienbereichen in einem oder mehreren Netzwerken berechtigt ist. Jeder Tivoli-Administrator wird durch ein Symbol auf der Tivoli-Arbeitsoberfläche dargestellt.

Tivoli Application Development Environment
Ein Tivoli-Toolkit, das die vollständige Anwendungsprogrammierschnittstelle (API) für Tivoli Management Framework enthält. Mit diesem Toolkit können Kunden und Tivoli-Partner ihre eigenen Anwendungen für die Tivoli-Umgebung entwickeln.

Tivoli Application Extension Facility
Ein Tivoli-Toolkit, mit dem Kunden das Leistungsspektrum der Tivoli-Anwendungen steigern können. Sie können beispielsweise einem Dialog Felder hinzufügen, benutzerdefinierte Attribute und Methoden für Anwendungsressourcen sowie benutzerdefinierte Symbole und Bitmap-Dateien erstellen.

Tivoli-Client
Siehe TMR-Client.

Tivoli Management Framework
Die Basissoftware, die zur Ausführung der Tivoli-Systemverwaltungsanwendungen erforderlich sind. Diese Softwareinfrastruktur ermöglicht die Integration von Tivoli-Systemverwaltungsanwendungen von Tivoli und von Tivoli-Partnern. Tivoli Management Framework umfasst Folgendes:

- Object request broker (oserv)
- Datenbank für verteilte Objekte
- Basisverwaltungsfunktionen
- Basisanwendungsdienste
- Basisdienste für die Arbeitsoberfläche wie die grafische Benutzerschnittstelle (GUI)

In einer Tivoli-Umgebung wird Tivoli Management Framework auf allen Clients und Servern installiert. Folgende Ausnahmen gelten: Tivoli Management Framework

wird niemals auf einem Client-PC installiert. Auf einem PC wird ein PC-Agent installiert. Nur der TMR-Server enthält die gesamte Objektdatenbank.

Tivoli Management Region (TMR)
In einer Tivoli-Umgebung ein Tivoli-Server und die ihm zugeordneten Clients. Eine Organisation kann über mehrere TMRs gleichzeitig verfügen. Eine TMR bezieht sich auf die tatsächliche physische Konnektivität, ein Richtlinienbereich dagegen auf die logische Anordnung der Ressourcen.

Tivoli NetWare Repeater (TNWR)
In einer Tivoli-Umgebung eine Serveranwendung, die auf einem Novell NetWare-Server installiert ist und eine Liste der verfügbaren Clients für den Server verwaltet. Der Tivoli NetWare Repeater führt zusammen mit der NetWare-verwalteten Station die Profilverteilung aus.

Tivoli SecureWay Security Manager
Software, die eine konsistente Definition, Implementierung und Durchsetzung von Sicherheitsrichtlinien in einer Network Computing-Umgebung ermöglicht.

Tivoli SecureWay User Administration
Ein Tivoli-Produkt, das eine grafische Benutzerschnittstelle (GUI) für die zentralisierte Verwaltung von Benutzer- und Gruppenkonten zur Verfügung stellt. Es ermöglicht die effiziente, automatisierte Verwaltung von Benutzer- und Systemkonfigurationsparametern, das sichere Delegieren von administrativen Tasks sowie die zentralisierte Steuerung aller Benutzer- und Gruppenkonten in einer Network Computing-Umgebung.

Tivoli-Server
Siehe TMR-Server.

Tivoli-Umgebung
Die auf Tivoli Management Framework basierenden Tivoli-Anwendungen, die bei einem bestimmten Kunden installiert sind und der Verwaltung des plattformübergreifenden Netzwerkbetriebs dienen. In einer Tivoli-Umgebung kann der Systemadministrator Software verteilen, Benutzerkonfigurationen verwalten, Zugriffsberechtigungen ändern, Vorgänge automatisieren, Ressourcen überwachen und Zeitpläne für Jobs erstellen.

TMR-Client
In einer Tivoli-Umgebung jeder Computer, mit Ausnahme des TMR-Servers, auf dem Tivoli Management Framework installiert ist. Ein TMR-Client führt oserv aus und verwaltet eine lokale Objektdatenbank. *Gegensatz* zu TMR-Server.

TMR-Server
In einer Tivoli-Umgebung der Server in einer Tivoli Management Region (TMR), auf dem das gesamte Tivoli-Softwarepaket gespeichert ist bzw. der auf dieses verweist, einschließlich der kompletten Objektdatenbank. *Gegensatz* zu TMR-Client.

TNWR

Siehe Tivoli NetWare Repeater.

Transaktion

Eine spezifische Gruppe von Eingabedaten, die die Ausführung eines bestimmten Prozesses oder Jobs auslöst; eine für ein Anwendungsprogramm bestimmte Nachricht.

V

Verwaltete Ressource

In einer Tivoli-Umgebung jede Hardware- oder Softwareentität (Maschine, Dienst, System oder Einrichtung), die durch ein Datenbankobjekt und ein Symbol auf der Tivoli-Arbeitsoberfläche dargestellt wird. Verwaltete Ressourcen müssen eine in einem Richtlinienbereich unterstützte Ressourcenart haben und unterliegen einem Regelsatz. Verwaltete Ressourcen umfassen verwaltete Knoten, Endpunkte, Task-Bibliotheken, Monitore, Profile und Schwarze Bretter.

Verwalteter Knoten

(1) In einer Tivoli-Umgebung jede verwaltete Ressource, auf der Tivoli Management Framework installiert ist und auf der oserv ausgeführt wird. (2) In der Internet-Kommunikation eine Workstation, ein Server oder ein Router mit einem Netzwerkverwaltungsagenten. Im Internet Protocol (IP) befindet sich auf dem verwalteten Knoten normalerweise ein Simple Network Management Protocol (SNMP)-Agent.

Verwaltungssystem für relationale Datenbanken (RDBMS)

Eine Gruppe von Hardware und Software, die den Zugriff auf eine relationale Datenbank ermöglicht und organisiert.

Virtuelle Anmeldung

Siehe Virtueller Benutzer.

Virtueller Benutzer

In Tivoli Management Framework eine Benutzer-ID, die verschiedenen tatsächlichen Benutzern in verschiedenen Arten von Architekturen zugeordnet werden kann. Beispielsweise kann der virtuelle Benutzer **$root_user** auf UNIX-Systemen dem Benutzer **root** und auf Windows NT-Systemen dem Administrator zugeordnet werden.

W

Weitergeben (Ausfüllen)

An ein Profil in einer Tivoli-Umgebung Informationen weitergeben (bzw. ein Profil mit Daten füllen), die an die zugehörigen verwalteten Ressourcen verteilt werden.

Windows NT-Repeater

In einer Tivoli-Umgebung die erste Windows NT-Maschine, auf der der Tivoli Remote Execution Service für Ausführungen auf fernen Systemen installiert ist. Während der Clientinstallation verteilt der NT-Repeater den Tivoli Remote Execution Service für Ausführungen auf einem fernen System mit Hilfe der Ausgabefächerung an alle anderen Windows NT-Clients.

Z

Ziel

Siehe Endpunkt.

Zuordnung der Benutzeranmeldung

In einer Tivoli-Umgebung die Zuordnung eines Anmeldenamens für einen Benutzer zu einem Benutzerkonto auf einem angegeben Betriebssystem. Die Zuordnung der Benutzeranmeldung ermöglicht Tivoli-Administratoren das Anmelden an der Tivoli-Umgebung oder das Ausführen von Vorgängen in der Tivoli-Umgebung mit einem einzigen Anmeldenamen, unabhängig von dem zur Zeit verwendeten System.

Index

A

Abrufen von Benutzerdatensätzen 262
AEF (AEF = application extension facility) 363
Anpassen
  Anzeigen hinzufügen 349
  Dialoge ändern 352
  Kategorien hinzufügen 347
  Kategorien löschen 350
  neue Attribute hinzufügen 351
  Unterkategorien hinzufügen 348
  Unterkategorien löschen 350
Anzeige des Benutzerprofils aktualisieren 256
Anzeigen
  Allgemeine OS/2-Anwendungen 413
  Anmelde-Workstations 416
  Identifikation 160
  NetWare-Anmeldeskript 204
  NetWare-Anmeldezeit 193
  NetWare-Anmeldung 190
  NetWare-E-Mail 202
  NetWare-fremde E-Mail 203
  NetWare-Gruppenzugehörigkeit 201
  NetWare-Kennwort 194
  NetWare-Netzwerkadresse 197
  NetWare-Sicherheit 201
  NetWare-Speicherplatzeinschränkungen auf Datenträgern 207
  NetWare-Verzeichnis 196
  NetWare-Workstations 208
  Optionen für OS/2-Konto 409
  OS/2-Gruppenzugehörigkeit 414
  OS/2-Konto 405
  Postadresse 161
  Subskribenten 161
  UNIX-Anmeldung 210
  UNIX-E-Mail 220
  UNIX-Kennwort 212
  UNIX-Verzeichnis 213
  Windows NT-Anmeldezeit 174, 182
Anzeigen *(Forts.)*
  Windows NT-Anmeldung 173, 181
  Windows NT-Fernzugriff 178, 188, 189
  Windows NT-Gruppenzugehörigkeit 177, 185
  Windows NT-Kennwort 175
  Windows NT-Verzeichnis 176, 184
  Windows NT-Workstations 177, 186
  Zuordnungen bei OS/2-Anmeldung 411
Auswerten
  Benutzerdatensätze 261
  Gruppendatensätze 324

B

Bearbeiten
  Benutzerdatensätze 231
  Gruppendatensätze 307
Beispiele
  Benutzer aus unterschiedlichen Abteilungen verwalten 40
  Benutzer in derselben Abteilung verwalten 38
  Benutzerprofile verteilen 26
Benutzer- und Gruppenverwaltung
  Einführung 1
  Funktionsweise 22
Benutzerdatensätze
  abrufen 262
  anzeigen 229
  auswerten 261
  automatisches Zusammenfügen während der Datenweitergabe 144
  bearbeiten 231
  Datensatzattribute sortieren 272
  eingeben
    allgemeine Informationen 160, 161

Benutzerdatensätze *(Forts.)*
eingeben *(Forts.)*
NetWare 190, 193, 194, 196, 197, 201, 202, 203, 204, 207, 208
UNIX 210, 212, 213, 220
Windows NT 173, 174, 175, 176, 177, 178, 181, 182, 184, 185, 186, 188, 189
erstellen 156
Kopien sperren 254
kopieren 249
löschen 236
mit Systemdateien synchronisieren 257
sortieren 270
sperren 231
suchen 223, 266
verschieben 252
zusammenfügen 234
Benutzerdatensätze kopieren 249
Benutzerdatensätze verschieben 252
Benutzerdatensätze zusammenfügen 234
Benutzerprofile
als verwaltete Ressourcen zuordnen 122
Anzeige aktualisieren 256
Beispiel für Verteilung 26
Einführung 23
erstellen 123
füllen, ausfüllen 144
klonen 126
löschen 129
planen 119
Richtlinien für Gültigkeitsprüfung definieren 138
Standardwerte für Verteilung festlegen 152
Standardwertegruppen definieren 132
verteilen 241
wechseln 268
Benutzersuchfunktion
Einführung 28
verwenden 223
Berechtigungsklassen 29, 31

C

CCMS 357
CLI-Befehle
wchkgrps 324
wchkusrs 260
wcpusr 251
wcrtgrp 307
wcrtprf 125, 128, 280, 282
wcrtusr 167, 171
wcrtusrcat 347
wcrtusrsubcat 348
wdel 131, 285
wdelgrp 312
wdelusr 237, 241
wdelusrcat 350
wdelusrsubcat 350
wdistrib 248, 318
wgetgrp 309
wgetpolm 136, 143, 290, 295
wgetprf, 265, 321
wgetusr 231
winstall 53
winstpw 69
wlspolm 136, 142, 290, 295
wmvusr 253
wpasswd 69, 83
wpopgrps 298
wpopusrs 151
wputdialog 349
wputpolm 136, 143, 290, 295
wrmusrg 310
wsetgrp 310
wsetnds 17, 146, 222, 242
wsetpr 123, 277
wsetusr 233, 255
wsetusrsubcat 348
wuninstpw 69
wvalidate 326

D

Datenlose Profilmanager 360
Dialoge
Benutzerprofile
Argumente des Richtlinienskripts 134
Attribute anzeigen 273

Dialoge *(Forts.)*
Benutzerprofile *(Forts.)*
Basisverzeichnis löschen 237
Datensatz suchen 267
Datensätze sortieren 271
Datensätze verschieben 253
Ergebnisse der Richtliniengültigkeits-prüfung 262
Profil ausfüllen 149
Profil klonen 128
Profil verteilen 245
Profildatensätze kopieren 250
Profile synchronisieren 259
Richtlinien für Gültigkeitsprüfung editie-ren 140
Richtlinienskript editieren 135
Standardwerte verteilen 153
Standardwertegruppen editieren 133
Subskriptionskopie abrufen 263
Zu Profil 269
Gruppenprofile
Argumente des Richtlinienskripts 287, 288
Attribute anzeigen 333
Datensatz suchen 327
Datensätze sortieren 331
Gruppenmerkmale 305
Gruppenprofilmerkmale 286
Profil ausfüllen 297
Profil erstellen 279
Profil klonen 282
Profil verteilen 315
Profildatensatz editieren 308
Profile synchronisieren 322
Richtlinien für Gültigkeitsprüfung editie-ren 292
Richtlinienskript editieren 289
Standardwerte verteilen 300
Standardwertegruppen editieren 287
Subskriptionskopie abrufen 320
Zu Profil 330
Domänen
als Endpunkte 404
OS/2 Warp-Server 418
verwalten 404
Domänencontroller 417

E

Erstellen
Benutzerdatensätze 156
Benutzerprofile 123
Gruppendatensätze 303, 304
Gruppenprofile 277

F

Fehlernachrichten 440
Fenster
Benutzerprofile
Benutzerprofilmerkmale 133
Profilmanager 124
Gruppenprofile
Profilmanager 284
Füllen, ausfüllen
Benutzerprofile 144
Einführung 25
Gruppenprofile 296
OS/2 404

G

Geänderte Benutzer-ID 419
Gruppendatensätze
Attribute sortieren 332
auswerten 324
bearbeiten 307
erstellen 303, 304
löschen 311
sortieren 330
suchen 326
Gruppenprofile
als verwaltete Ressourcen zuordnen 276
Einführung 23
erstellen 277
füllen, ausfüllen 296
klonen 280
Kopien abrufen 318
löschen 283

Gruppenprofile *(Forts.)*
mit Systemdateien synchronisieren 321
Richtlinien für Gültigkeitsprüfung definieren 291
Standardwerte für Verteilung festlegen 299
Standardwertegruppen definieren 286
verteilen 313
wechseln 329

I

Identifikationsanzeige 160
Installations-Repository 48
Installieren
AS/400-Pakete 61
LDAP-Pakete 56
OS/2-Pakete 59
Tivoli User Administration 49
Tivoli User Administration, Gateway-Paket 53
wpasswd (Befehl) 69

K

Kennwörter 85
'wpasswd' verwenden 84
ändern 83, 102
Berechtigungsklassen für Änderungen 86
geändert unter OS/2 419
lange Kennwörter 110
Leistungsspektrum von wpasswd 101
nicht vorhanden 418
Qualitätsregeln 92
Kennwörter zu ändern 83
Klonen
Benutzerprofile 126
Gruppenprofile 280

L

Löschen
Benutzerdatensätze 236
Benutzerprofile 129
Gruppendatensätze 311
Gruppenprofile 283

N

Nachrichten 440
NETAPI32.DLL, Bibliothek 418
NetWare-Anzeigen
Anmeldeskript 204
Anmeldezeit 193
Anmeldung 190
Datenträgereinschränkungen 207
E-Mail 202
fremde E-Mail-Adressen 203
Gruppenzugehörigkeit 201
Kennwort 194
Netzwerkadresse 197
Sicherheit 201
Verzeichnis 196
Workstations 208
NetWare-Endpunktkommunikation 17

O

Oneshot-Attribute 367
OS/2-Anzeigen
Anmelde-Workstations 416
Anmeldezuordnungen 411
Anwendungen 413
Gruppenzugehörigkeit 414
Konto 405
Kontooptionen 409
OS/2-Endpunkte 417

P

Postadresse (Anzeige) 161
Produktgeschichte 356
Profile
  Benutzer und Gruppe, Einführung 23
  bereichsübergreifende Unterstützung 23
  datenlose Profilmanager 360
  Einzelheiten, die erläutert werden 358
  füllen, ausfüllen 25
  Namenskonventionen 119
  Profilmanager 359
  Richtlinien 24
  Subskribenten 359
  verteilen 26

R

Richtlinien 24
Richtlinien für Gültigkeitsprüfung
  definieren 138, 291
  Skriptargumente editieren 141
  verwenden 261, 324

S

SERVERS, Gruppenkonto 419
Sicherheitsverwaltung 29
  siehe auch Berechtigungsklasse 29
SIS, siehe Software Installation Service> 48
Sortieren
  Attribute von Gruppendatensätzen 332
  Benutzerdatensätze 270
  Datensatzattribute 272
  Gruppendatensätze 330
Sperren
  Kopien von Benutzerdatensätzen 254
  während der Bearbeitung 231
Standardwertegruppen
  bereits festgelegt 157
  definieren 132, 286
  Skriptargumente editieren 134
Subskribenten
  auf Datensatzebene 361
  auf Datensatzebene festlegen 161
  Datensatzebene 24
  des Profilmanagers 359
  Profilmanager 24
Subskriptionen auf Datensatzebene 161
Suchen
  Benutzerdatensätze 266
  Gruppendatensätze 326
Synchronisieren
  Benutzerdatensätze mit Systemdateien 257
  Gruppenprofile mit Systemdateien 321

T

Task-spezifische Berechtigungsklassen 31
Tivoli SecureWay Security Management, Integration mit 29
Tivoli User Administration aktualisieren 70
Tivoli User Administration deinstallieren 72

U

UNIX-Anzeigen
  Anmeldung 210
  E-Mail 220
  Kennwort 212
  Verzeichnis 213

V

validate (Befehl) 326
Verteilen
  an OS/2-Endpunkte 418
  Benutzerprofile 241
  Gruppenprofile 313
  OS/2 404
  Standardeinstellungen festlegen 152, 299

Verteilen *(Forts.)*
Verteilungsverarbeitung und Kennwörter 365
Verwaltete Ressourcen
Benutzerprofile zuordnen 122
Gruppenprofile zuordnen 276
Verwaltung
Benutzer und Gruppen 1, 22
Sicherheit 29

W

waddprop (Befehl) 378
waddusrprop (Befehl) 378
wchkgrps (Befehl) 324
wchkusrs (Befehl) 260
wcpusr (Befehl) 251
wcrtgrp (Befehl) 307
wcrtprf (Befehl) 125, 128, 280, 282
wcrtusr (Befehl) 167, 171
wdel (Befehl) 131, 285
wdelgrp (Befehl) 312
wdelusr (Befehl) 237, 241
wdistrib (Befehl) 248, 318
wgenusrdef (Befehl) 379
wgetgrp (Befehl) 309
wgetpolm (Befehl) 136, 143, 290, 295
wgetprf (Befehl) 265, 321
wgetusr (Befehl) 231
Windows NT
Domänenverwaltung 9
Windows NT-Anzeigen
Anmeldezeit 174, 182
Anmeldung 173, 181
Fernzugriff 178, 188, 189
Gruppenzugehörigkeit 177, 185
Kennwort 175
Verzeichnis 176, 184
Workstations 177, 186
winstall (Befehl) 53
winstpw (Befehl) 69
wlspolm (Befehl) 136, 142, 290, 295
wmvusr (Befehl) 253
wpasswd (Befehl) 69, 83, 84, 101
wpopgrps (Befehl) 298
wpopusrs (Befehl) 151
wputpolm (Befehl) 136, 143, 290, 295
wrmusrg (Befehl) 310
wsetgrp (Befehl) 310
wsetnds (Befehl) 17, 146, 222, 242
wsetpr (Befehl) 123, 277
wsetusr (Befehl) 233, 255
wuninstpw (Befehl) 69

GC12-2982-01